JOINT FORCES STAFF COLLEGE
JOINT ADVANCED WARFIGHTING SCHOOL

THE IMPACT OF ORGANIZATIONAL CULTURE ON THE SHARING OF HOMELAND SECURITY INFORMATION

By

Jeffery E. Bradey
GS-15, Department of Defense

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

Signature: _____

4 April 2008

Thesis Adviser: William T. Eliason, Colonel, USAF

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-06-2008	Master's Thesis	23-07-2007 to 13-06-2008

4. TITLE AND SUBTITLE
THE IMPACT OF ORGANIZATIONAL CULTURE ON THE SHARING OF HOMELAND SECURITY INFORMATION

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Jeffery E. Bradey

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Forces Staff College
Joint Advanced Warfighting School
7800 Hampton Blvd.
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER

JFSC 25789

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This thesis identifies problems that have impacted the implementation of the Homeland Security Information Network. These problems have ranged from programmatic to legal to cultural issues. The Department of Homeland Security has addressed several of the problems impacting the Homeland Security Information Network. The Department of Homeland Security established a program management office and a privacy office to resolve some of the challenges to the Homeland Security Information Network program. The clash of cultures is often discussed in relation to mergers and acquisitions in the business world. This phenomenon has been exhibited by participants in homeland security information sharing during the deployment of the Homeland Security Information Network. Solving these cultural problems requires cooperation and buy-in from the senior leadership of the Department of Homeland Security to the end users of the Homeland Security Information Network in the federal, state, and local governments. Finding a technique to effect meaningful culture change in the homeland security community is the key to making the Homeland Security Information Network a viable information sharing tool.

15. SUBJECT TERMS
organizational culture, Homeland Security Information Network, information sharing

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	Unclassified Unlimited	77	**19b. TELEPHONE NUMBER** *(include area code)* 757-443-6301

Standard Form 298 (Rev. 8-98)

Abstract

This thesis identifies problems that have impacted the implementation of the Homeland Security Information Network. These problems have ranged from programmatic to legal to cultural issues. The Department of Homeland Security has addressed several of the problems impacting the Homeland Security Information Network. The Department of Homeland Security established a program management office and a privacy office to resolve some of the challenges to the Homeland Security Information Network program. The clash of cultures is often discussed in relation to mergers and acquisitions in the business world. This phenomenon has been exhibited by participants in homeland security information sharing during the deployment of the Homeland Security Information Network. Solving these cultural problems requires cooperation and buy-in from the senior leadership of the Department of Homeland Security to the end users of the Homeland Security Information Network in the federal, state, and local governments. Finding a technique to effect meaningful culture change in the homeland security community is the key to making the Homeland Security Information Network a viable information sharing tool.

Table of Contents

I. Introduction

The Homeland Security Act of 2002, which established the Department of Homeland Security, mandated homeland security information sharing. Recognizing the need to fill a void in the sharing of terrorism information at the federal, state and local levels; the Department of Homeland Security stood up the Homeland Security Information Network (HSIN). This system leveraged an existing information system developed by state and local officials in cooperation with the federal government. The Department of Homeland Security has faced numerous problems with its implementation of the Homeland Security Information Network. These problems have ranged from technical to programmatic to legal. This author asserts that there is one problem greater than each of these – cultural differences among organizations using the HSIN.

This author contends that the organizational cultural differences among the homeland security community[1] are the primary impediment to realizing the goals of the Homeland Security Information Network. The goals of the Homeland Security Information Network are providing situational awareness, facilitating information sharing and collaboration with homeland security partners, providing advanced analytic capabilities, and enabling real time sharing of threat information.[2]

The Homeland Security Act of 2002 mandated the sharing of homeland security information. As a means to satisfy the legal requirements to implement information sharing among Federal agencies and appropriate state and local organizations, the use of

---

[1] The term "homeland security community" is defined as federal, state, and local organizations with the mission of homeland security. Members of the homeland security community include the Department of Homeland Security, the Federal Bureau of Investigation, state homeland security organizations, and state and local law enforcement agencies.

[2] U.S. Department of Homeland Security, "Homeland Security Information Network," http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm (accessed September 9, 2007).

HSIN to exchange terrorism information is critical to prevent further acts of terrorism within the U.S. The 9/11 Commission identified the need to consolidate information in a "network-based information sharing system that transcends traditional governmental boundaries."[3] Identifying the cultural differences among organizations and analyzing their causes will form a foundation of understanding necessary to improve the symptoms of the cultural differences.

This thesis will review the background of the HSIN. It will show the evolution from a previously existing system, the Joint Regional Information Exchange System. Key legislation impacting the HSIN such as the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 will be presented as well as significant milestones that drove the Department of Homeland Security's deployment of the HSIN. The National Strategy for Homeland Security will be discussed to demonstrate the necessity of the HSIN to solve the problems of homeland security made obvious by 9/11.

The key challenges that have affected the implementation of the HSIN will be discussed. Some of these problems include the lack of an enterprise architecture, inadequate acquisition policies, legal issues restricting information sharing, and organizational culture differences within the homeland security community.

This thesis will then argue that the differing cultures of the homeland security community have been the primary roadblock to achieving the goals of HSIN. These cultural differences are rooted in the way each of the organizations has evolved and what

[3] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report Executive Summary*, http://www.9-11commission.gov/report/911Report_Exec.pdf (accessed September 9, 2007), 21.

their missions are. Factors such as federalism, trust, need-to-know, and funding have influenced each culture.

To overcome the impediments to HSIN's planned use, recommendations on how to mitigate the impacts of culture and modify the collective homeland security culture will be presented. These recommendations will require change at the federal, state, and local levels. Because of its role in this unique confederation of organizations, this thesis will demonstrate that the Department of Homeland Security has an important opportunity to improve the utility of HSIN and its contribution to the war on terrorism.

II. Background

Following the events of September 11, 2001, it became obvious that the federal government needed to better coordinate its efforts against terrorism in the United States. There was a need to develop a plan for homeland security in the United States, a plan that ensured America was prepared to protect its citizens and defend its borders. The executive branch of the federal government was aware that action was necessary to focus its efforts and restore public confidence.

The need to share intelligence was not a new concept. Since the 1990's, Congress has sought to make statutory changes to aid in information sharing. This was driven by the belief that mutual benefit would be obtained by sharing information as international crime and terrorism expanded into the sphere of law enforcement. This information could no longer be treated exclusively as foreign intelligence. Several bills were introduced in Congress to facilitate this information sharing but each was defeated because of concerns about the risks to civil liberties.

After 9/11, it became apparent that more information sharing needed to take place between law enforcement and the Intelligence Community but with safeguards in place to protect civil liberties and the criminal justice system. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intersect and Obstruct Terrorism (USA PATRIOT) Act of 2001, signed into law on October 26, 2001, was the first legislation to address increased information sharing. The USA PATRIOT Act encouraged cooperation between the Intelligence Community and law enforcement. For the Intelligence Community, it also expanded access to information gathered in criminal

investigations. Congress and the American people were now ready to make information sharing a weapon against terrorism.

On October 8, 2001, President George W. Bush created the Office of Homeland Security to "coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[1] The Office of Homeland Security's initial task was to produce the first National Strategy for Homeland Security. One of the key topics to be included in the strategy would be the recommendation to Congress to create a new executive department for homeland security. The President presented the National Strategy for Homeland Security to Congress on July 16, 2002.

The National Strategy for Homeland Security (NSHS) organized the nation's efforts against terrorism. The strategy provided direction for each federal department and agency with a homeland security mission. Roles for the state and local governments were also included in the strategy. The strategy identified several different areas where information sharing could be improved. Two of these areas were laws and information sharing systems. Statutes were needed to streamline information sharing among intelligence and law enforcement agencies at the federal level. Because of the terrorism threat, restrictions that had impeded information sharing in the past were no longer accepted without question. In addition, information sharing systems need to be integrated across the federal government and also across state and local governments.[2] Since the

---

[1] Executive Order no. 13228, Code of Federal Regulations, title 3, p. 796 (2001), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_cfr_3v1&docid=3CFR13228.pdf (accessed January 4, 2008).

[2] President, *National Strategy for Homeland Security*, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (accessed August 4, 2007): xi.

federal, state, and local governments each had a role in homeland security; information sharing systems had to ensure that all appropriate government entities had access to the terrorism information relevant to their organization.

In the National Strategy for Homeland Security, existing information systems were identified as deficient for "supporting the homeland security mission. Databases used for federal law enforcement… [and] … intelligence… have not been connected in ways that allow us to comprehend where information gaps or redundancies exist… we must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy."[3] The National Strategy for Homeland Security acknowledged the complexity of interconnecting systems at the federal, state, and local levels in a coordinated, non-duplicative manner. It also clearly stated the importance of both vertical and horizontal information sharing.[4] The strategy had addressed the priorities for the proposed Department of Homeland Security. The President looked to Congress to put the strategy into action with legislation to create a new executive department for homeland security.

The Homeland Security Act of 2002, enacted on November 25, 2002; created the Department of Homeland Security (DHS). The Homeland Security Act defined the department's mission as "prevent terrorist attacks within the United States; reduce the vulnerability of the United States to terrorism; minimize the damage, and assist in the

---

[3] President, *National Strategy for Homeland Security*, xi.

[4] Vertical information sharing is information sharing among different levels of government while horizontal information sharing is at the same level of government. For example, information sharing between the FBI and the Maryland State Police is vertical information sharing and between DHS and the FBI is horizontal information sharing.

recovery, from terrorist attacks that do occur within the United States."[5] One of the primary functions of the new department was "coordination with other parts of the federal government, with state and local governments, and with the private sector" [6] on homeland security issues. The Homeland Security Act established the department's entitlement to receive intelligence relating to threats of terrorism from agencies and departments of the federal government. DHS is also responsible to ensure that terrorism-related intelligence that it has access to will be shared with the federal, state, and local governments. Information sharing with the Department of Homeland Security by the state and local governments was encouraged by the Homeland Security Act. These authorities were given to DHS so it could fulfill its mission of analyzing terrorist threat information. The Homeland Security Act also mandated that "all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared."[7] The directive had been given for the Department of Homeland Security to build an information sharing system for use by federal, state, and local governments.

President Bush issued Executive Order 13311 on July 29, 2003, delegating responsibility to the Secretary of Homeland Security to prescribe and implement the information sharing procedures that were called out in the Homeland Security Act. The

---

[5] Homeland Security Act of 2002, Public Law 107-296, http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.181&filename=publ296.pdf&directory=/diska/wais/data/107_cong_public_laws (accessed September 2, 2007) §101.

[6] Executive Office of the President, "Analysis For The Homeland Security Act of 2002," http://www.whitehouse.gov/deptofhomeland/analysis/hsl-bill-analysis.pdf (accessed September 16, 2007), 2.

[7] Homeland Security Act, §892b.

procedures would dictate how relevant homeland security information would be shared within the federal government and with the state and local governments. The Department of Homeland Security now had complete authority over the entire process; developing the procedures to share homeland security information and implementing an information sharing system to facilitate dissemination of the information. DHS now needed to begin the planning and implementation of an information sharing system. With its strategy defined by the National Strategy for Homeland Security and its mission and authorities relating to information sharing granted by the Homeland Security Act and the President, the department began to address its diverse set of responsibilities.

In the three years after 9/11, there were considerable resources dedicated to investigating why America was unprepared for the terrorist attacks on September 11, 2001. The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence set up a joint inquiry to investigate what the Intelligence Community knew regarding a terrorist threat prior to the attacks. In the declassified findings of the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 released in December 2002, the Joint Inquiry found that

> serious problems in information sharing also persisted, prior to September 11, between the Intelligence Community and relevant non-Intelligence Community agencies. This included other federal agencies as well as state and local authorities. This lack of communication and collaboration deprived those other entities, as well as the Intelligence Community, of access to potentially valuable information in the "war" against Bin Ladin.[8]

[8] House Permanent Select Committee on Intelligence. *Report of the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*. 107th Cong., 2d sess., December 2002, http://www.gpoaccess.gov/serialset/creports/pdf/fullreport_errata.pdf (accessed November 17, 2007), 84. Subsequently in this paper, this inquiry will be referred to as the "Joint Inquiry."

President Bush and Congress established the National Commission on Terrorist Attacks Upon the United States[9] in November 2002 to build upon the Joint Inquiry's findings. The 9/11 Commission looked beyond the Intelligence Community in its review. The 9/11 Commission was also directed to investigate law enforcement agencies, diplomacy, immigration, the flow of assets to terrorists, immigration, Congressional oversight, and other areas determined relevant to the Commission.[10]

There was a body of evidence mounting that the attacks of 9/11 were successful because of poor information sharing among the intelligence agencies as well as other federal agencies and state and local governments. With the mandate from the Homeland Security Act, as well as Congressional findings, to share homeland security information, and the National Strategy for Homeland Security providing the vision for the nation; the Department of Homeland Security needed to move quickly to improve information sharing.

Among the first initiatives that DHS undertook to improve information sharing was the Homeland Security Information Network. This computer system leveraged an existing system, the Joint Regional Information Exchange System (JRIES), to share terrorism information. Under the new moniker, Homeland Security Information Network, the JRIES system would be expanded to all 50 states, five territories, and 50 major urban areas. JRIES was deployed in February 2003 as a pilot system to connect the California Anti-Terrorism Center, the New York Police Department, and the Defense

[9] The more commonly used name for the commission is the 9/11 Commission. Additional references in this paper will use this designation as well.

[10] Intelligence Authorization Act for Fiscal Year 2003, Public Law 107-306, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ306.107.pdf (accessed October 23, 2007) §602.

Intelligence Agency. The system was designed to "facilitate the exchange of suspicious activity reports, register events potentially related to terrorist activity, and foster real-time intelligence and law enforcement collaboration in a secure environment across federal, state, and local jurisdictions."[11]

In September 2003, the Defense Intelligence Agency turned over responsibility for JRIES to the Department of Homeland Security because of budget issues. After taking over JRIES, DHS saw the potential of the system as a solution for the department's information sharing and communication requirements. Because of its increased scope as the "primary communication, collaboration, situational awareness, and information-sharing system"[12] for DHS, the department renamed the system the Homeland Security Information Network. On February 24, 2004, Secretary of Homeland Security Tom Ridge formally announced the creation of the Homeland Security Information Network (HSIN).

HSIN provides real-time information sharing using secure Internet-based technology. HSIN connects its users with the National Operations Center,[13] which maintains situational awareness of the security of the homeland and coordinates communication among homeland security partners. Data exchanged on the Homeland Security Information Network is at the sensitive but unclassified classification level. HSIN focuses on information exchange and real-time collaboration. The network includes information analysis tools to support collaborative analysis and reporting across

---

[11] U.S. Department of Homeland Security, Office of Inspector General, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-38_Jun06.pdf (accessed August 10, 2007), 7.

[12] U.S. Department of Homeland Security, OIG-06-38, 8.

[13] Formerly known as the Homeland Security Operations Center.

federal, state, and local users.[14] The initial Homeland Security Information Network users included state homeland security advisers, state National Guard offices, state emergency operations centers, and local emergency services (law enforcement and fire departments). The users were provided software, hardware, and training to connect to and use the system. This connectivity enhanced information sharing and situational awareness as an expanded subset of the homeland security community could now use HSIN to exchange data. Plans for subsequent deployments targeted over 3000 counties across the U.S.

Also, on February 24, 2004, the Department of Homeland Security's first strategic plan was issued. Two of the seven goals of the Department of Homeland Security could be directly tied to the new Homeland Security Information Network's objective. The goal of awareness – obtaining intelligence and analyzing threats, and the goal of prevention – deterring and mitigating threats to America, had subordinate objectives that called for developing capabilities to support information analysis and sharing. The Homeland Security Information Network was a priority for the department to accomplish their mission.

The most incriminating report about the government's actions leading up to September 11, 2001 was the 9/11 Commission Report. This report was issued publically on July 22, 2004. The commission found that information sharing needed to be improved and moved from a culture of "need-to-know" to a culture of "need-to-share." The commission also recommended that "legal, policy, and technical issues across agencies

[14] Richard A. Russell, "Department of Homeland Security: Information Sharing," (brief presented at 2004 Symposium on Integrated Justice Information Systems Supporting the Homeland, Washington DC, March 22, 2004) http://www.search.org/conferences/2004symposium/presentations/monday/homeland.ppt (accessed August 2, 2007)

[be resolved] to create a trusted information network."[15] This finding was aimed at the federal government as a whole. The guidance from the 9/11 Commission was to eliminate the barriers to sharing information needed by the government to protect its citizens from terrorism.

The Intelligence Reform and Terrorism Prevention Act of 2004 was Congress' response to the 9/11 Commission Report. This legislation was the next step to improving information sharing. While targeting primarily the Intelligence Community through its reform, the Intelligence Reform and Terrorism Prevention Act (IRTPA) continued to promote collaboration of the Intelligence Community with other federal agencies and departments. IRTPA specifically focused on improving terrorism information sharing through the establishment of the Information Sharing Council and the Information Sharing Environment. The message, clearly stated in the Homeland Security Act, the Intelligence Reform and Terrorism Prevention Act, and several executive orders; was that information sharing and systems to promote information sharing were paramount to the prevention of future terrorist attacks.

The federal government has taken considerable strides to address the information sharing problems highlighted by the events of 9/11. The President stood up the Office of Homeland Security to develop "a comprehensive national strategy to secure the U.S. from terrorist threats and attacks."[16] Congress enacted legislation to facilitate information sharing, establish the Department of Homeland Security and give it

---

[15] National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. http://www.9-11commission.gov/report/911Report.pdf (accessed September 9, 2007), 418.

[16] Executive Order no. 13228.

responsibility for terrorism information sharing, and reorganize the Intelligence Community – all with the goal of better information sharing.

The Department of Homeland Security leveraged an existing system to satisfy the Congressional mandate to share terrorism information. Within a year of the announcement of the Homeland Security Information Network, reports began appearing highlighting the lack of progress made on the program. The majority of these reports were issued by the U.S. Government Accountability Office (GAO). The GAO identified that homeland security information sharing was a high risk area because minimal progress had been made on the information sharing procedures and the existence of a large number of duplicative systems, all with the function of information sharing.[17] Many of the issues, while they were external to the HSIN program, were still a DHS responsibility. Establishing information sharing procedures and developing an enterprise architecture for the department were some of the issues.

The Department of Homeland Security Office of the Inspector General also presented findings that detailed some of the causes of the delays. In the Inspector General's report to Congress, many of the delays were blamed on the haste to deploy an information sharing capability. These shortcuts affected the efficacy of the Homeland Security Information Network by failing to conduct comprehensive planning. Minimal coordination with Homeland Security Information Network users also affected the system implementation. These problems were endemic to the newly established Department of Homeland Security. The lack of progress on the Homeland Security Information Network can be partially attributed to the accelerated schedule, but there are other issues

[17] U.S. Government Accountability Office, *Information Technology: Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives*, GAO-07-822T. http://www.gao.gov/new.items/d07822t.pdf (accessed August 2, 2007), i.

that have contributed to HSIN's current state. These problems have been grouped into programmatic, legal, and cultural issues. These issues and their impacts will be assessed in the next chapter and updated with the progress to date.

III. HSIN Problems

While HSIN has achieved some success since its announcement in 2004 and subsequent deployment, there have been several aspects that have impeded the progress and maturation of the system. The three primary areas impacting the Homeland Security Information Network are programmatic, legal, and cultural. Each of these areas is worthy of substantial study but will only be covered to the detail necessary to examine the extent of impact in each area. None of the impacts in these areas have been significant enough to negate the utility of HSIN but each has delayed the early, optimistic goals for the Homeland Security Information Network.

Programmatic Issues

Programs are typically initiated with the identification of a user need. The need for an information sharing system was recognized and issued as a legislative mandate in the Homeland Security Act. DHS was the executive department with the requirement to build this system for sharing terrorism-related information. In the quest to deploy a system to meet the informational needs of the homeland security community and with a heightened threat level in the U.S., the Department of Homeland Security accelerated the schedule of HSIN. The initial schedule established a completion date of December 2004 for installing the system and training users in all fifty states, fifty cities, and five U.S. territories. In its attempt to maintain the schedule, the HSIN program management ignored many key planning steps recognized as necessary for the successful execution of a program. This accelerated schedule subsequently created a domino effect for the problems in the HSIN program. Shortcuts taken in the initial phases set the program up for subsequent problems. Issues that will be discussed in the programmatic area are the

systems engineering process, the DHS enterprise architecture, and the department's acquisition processes.

System Engineering

Due to the accelerated schedule for HSIN, the program management did not use accepted system engineering practices to plan, design, and implement HSIN. Systems engineering is the process applied to transition from a stated capability need to an operationally effective and suitable system.[1] Requirements definition is an early key step in the systems engineering process that lays the groundwork for project success. Requirements are the driving force of the program. The requirements process develops the functions that must be performed by the system. The requirements process requires user involvement to establish priorities for the functions that the system will perform. These priorities will drive the system design. Without user input, the system is unlikely to meet the users' needs, i.e. it cannot perform the functions it was intended to do.

The Office of Management and Budget provides guidance to the federal agencies to involve the users in IT system design to reduce project risk.[2] User engagement was largely ignored early in the HSIN program, so the system requirements were incomplete at best. In June 2006, DHS acknowledged in an Inspector General report on HSIN that its "efforts to obtain input and address requirements from all HSIN user communities were inadequate."[3]

---

[1] U. S. Department of Defense, "Defense Acquisition Guidebook," https://akss.dau.mil/dag/GuideBook/PDFs/Chapter_4.pdf (accessed December 6, 2007) §4.1, 2.

[2] U.S. Office of Management and Budget, "Circular A-11 Part 7, Planning, Budgeting, Acquisition, and Management of Capital Assets," http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf (accessed November 21, 2007), 6.

[3] U.S. Department of Homeland Security, OIG-06-38, 9.

Another important reason to engage the users is to understand what systems they currently use. This information will give the program management insight into whether the existing systems will be integrated with the new system to retain functionality or the new system will be built with the existing functionality as a requirement. The Government Accountability Office published a report in 2004, which exhibited the importance of understanding the functionality of existing systems. GAO found that there were 25 operational systems and more than 100 major applications in the federal government that supported homeland security missions at the unclassified and sensitive but unclassified levels.[4] The possibility that duplication existed among these systems was likely and further put HSIN's primary function, information sharing, at risk because users were unsure of which system to use. Duplication of effort will also be discussed in more depth in the next section on enterprise architecture.

In the systems engineering process, a concept of operations (CONOP) should be developed, subsequent to the requirements definition, to understand how the users will employ the system. A concept of operations would allow the designers to put the requirements into an operational context. The first concept of operations for HSIN was written 18 months after the program was started. Even then, the CONOP did not provide sufficient detail for each of the user communities.[5] In the system engineering process after requirements are developed and a system is built, metrics are used to evaluate how well a system satisfies its requirements. The metrics must be meaningful, capturing how well the system is performing against its standard – the specifications, which are derived

[4] U.S. Government Accountability Office, *Information Technology: Major Federal Networks That Support Homeland Security Functions*, GAO-04-375. http://www.gao.gov/new.items/d04375.pdf (accessed September 2, 2007), 2.

[5] U.S. Department of Homeland Security, OIG-06-38, 12.

from user requirements. The Government Performance and Results Act of 1993 and the Clinger-Cohen Act of 1996 require performance measures in information technology programs to measure how well the desired outcome has been achieved. The circumstances of the HSIN program mirror typical problems associated with programs that have not employed a disciplined systems engineering approach. Systems engineering emphasizes that decisions made early in the life of a program can have great impact on the effectiveness and total cost of the system. HSIN embodies the approach of "deliver it now and fix it later."[6] Indicative of the systems engineering failures is the migration from HSIN's original software platform to a web portal approximately one year after HSIN was introduced. The reason for the migration was a lack of capacity in the original software. This lack of capacity would have been addressed up front if the program management and systems engineering processes had been fully utilized.

Enterprise Architecture

As early as January 2003, the Government Accountability Office identified the Department of Homeland Security's implementation and transformation as a high risk area.[7] The activity of developing an enterprise architecture is especially critical to DHS as it transforms itself from 22 separate agencies into an integrated executive department. In addition to the benefits of transforming DHS, developing an enterprise architecture was critical to understanding how to address information sharing with all levels of government and implement its new information sharing system, HSIN.

---

[6] Benjamin S. Blanchard and Wolter J. Fabrycky, *Systems Engineering and Analysis*, 3rd ed. (Upper Saddle River, NJ: Prentice-Hall, 1998) 37.

[7] U.S. General Accounting Office, *High-Risk Series: An Update*, GAO-03-119. http://www.gao.gov/pas/2003/d03119.pdf (accessed October 14, 2007), 18.

An enterprise architecture is defined as "a blueprint that defines… how an organization's information technology (IT) systems operate today, how they are to operate in the future, and a road map for the transition."[8] To understand the significance of the enterprise architecture requires examination of its definition. The baseline ("as-is") architecture is the current inventory of IT systems, processes, and procedures. The target ("to be") architecture is the organization's desired end state for its IT systems and processes. The transition strategy is the plan to move from the baseline architecture to the desired end state or target architecture within a certain timeframe. The transition strategy links organizational investment to the target architecture. This strategy also sets priorities for the transitional programs and projects.[9]

The information in the enterprise architecture provides a clear picture of the new solutions needed to reach the enterprise architecture end state. This information gives decision makers pertinent information to evaluate new programs in the context of the target architecture. By consolidating all organizational information, the enterprise architecture reduces duplicative systems and improves business processes.[10] With an enterprise architecture in place, a more coherent picture of the plans and activities that require resources can be presented. The architecture maximizes the investments made by an organization to achieve its mission. While critical to IT resources in an organization, an enterprise architecture can be used as a roadmap to transform an organization through

---

[8] U.S. Government Accountability Office, "Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains," GAO-04-777. http://www.gao.gov/new.items/d04777.pdf (accessed July 31, 2007), 1.

[9] U.S. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *FEA Practice Guidance*, http://www.whitehouse.gov/omb/egov/documents/FEA_Practice_Guidance.pdf (accessed September 23, 2007), 4-1.

[10] U.S. Government Accountability Office, GAO-04-777, 12.

changes in business processes, organizational structure, and IT resources. The use of an enterprise architecture helps an organization understand how to improve processes and perform functions more efficiently. An enterprise architecture is a transformation enabler. If implemented properly, an enterprise architecture "eliminates duplication, promotes interoperability, reduces costs, and optimizes mission performance."[11] In February 2004, the chief information officer of the Department of Homeland Security, who is responsible for the developing the enterprise architecture, said his first priority was "two-way information sharing down to the state and local community level."[12]

The development of a DHS-wide enterprise architecture afforded the department the opportunity to "identify common activities that facilitate the collaboration and exchange of homeland security information [and] implement policy related to the homeland security community."[13] DHS issued its first version of an enterprise architecture in September 2003. This plan was made without the benefit of a DHS strategic plan, which handicapped building a target architecture and transition plan. DHS' initial enterprise architecture submission was described as "a partial basis upon which to build future versions."[14] DHS continued to refine its enterprise architecture based on GAO's 2004 assessment of the department's initial enterprise architecture. With an IT budget of approximately $297 million for fiscal year 2006 and an evolving enterprise architecture, DHS' plan of IT expenditures was unclear. Congress wanted

---

[11] U.S. Government Accountability Office, GAO-04-777, 2.

[12] Henry S. Kenyon, Maryann Lawlor, and Cheryl Lilie, "Breaking Down Barriers to Homeland Security," *Signal* 58, no. 9 (May 2004): 77.

[13] Interoperability Clearinghouse Architecture Resource Center, "Homeland Security Enterprise Architecture," Homeland Security Brief to Industry Advisory Council on December 5, 2003, http://www.ichnet.org/IAC%201252003.ppt (accessed July 31, 2007), 26.

[14] U.S. Government Accountability Office, GAO-04-777, 2.

insight into the alignment of DHS' IT expenditures with its enterprise architecture. As leverage to get this information from DHS, Congress mandated in the DHS Appropriations Act of 2006 that the DHS chief information officer (CIO) provide a report including an enterprise architecture and a capital investment plan for implementing that enterprise architecture.[15] This requirement showed Congress' recognition of the importance of an enterprise architecture to transform DHS, manage the department's IT expenditures, and improve information sharing within the homeland security community. The CIO issued the department's latest enterprise architecture, EA 2006, in response to the DHS Appropriation Act requirement to produce an enterprise architecture and a capital investment plan for implementing that enterprise architecture. GAO reviewed EA 2006 and rated it fifth of 27 in the federal government for maturity but stated that the enterprise architecture was "still not sufficiently complete and usable… [and] did not fully address the range of stakeholder comments."[16]

The information used to develop the enterprise architecture was not complete enough early in the HSIN program to understand the relationships and duplication of functions among other information sharing systems such as the Department of Justice's Law Enforcement Online (LEO) and the Regional Information Sharing System (RISS), a state and local government initiative. If developed properly, an enterprise architecture helps reduce duplication of functions through its comprehensive inventory of systems,

---

[15] Department of Homeland Security Appropriations Act, 2006, Public Law 109-90, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ090.pdf (accessed November 18, 2007), Title I.

[16] U.S. Government Accountability Office, *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation*, GAO-06-831. http://www.gao.gov/new.items/d06831.pdf (accessed July 31, 2007), 31; U.S. Government Accountability Office, *Homeland Security: DHS Enterprise Architecture Continues to Evolve but Improvements Needed*, GAO-07-564. http://www.gao.gov/new.items/d07564.pdf (accessed July 31, 2007), 3.

applications, and processes. An enterprise architecture also promotes interoperability through the documentation of system interconnections, data flows, and the inventory of systems, applications, and processes. Since this inventory was not done, no one really understood how HSIN's capabilities matched up to other systems. This approach failed to utilize synergies between HSIN and other existing information sharing systems in the law enforcement and homeland security communities.

In addition to the tangible benefits of implementing an enterprise architecture, the Clinger-Cohen Act of 1996 requires the federal government to employ enterprise architectures with the goal of improving the way the federal government procures and manages information technology resources. To realize this improvement, the Clinger-Cohen Act calls for the "implementation of a sound and integrated information technology architecture for the executive agency."[17] The Office of Management and Budget (OMB) was assigned responsibility to ensure federal agencies adhered to the Clinger-Cohen Act. OMB issued Circular A-130 as guidance to federal agencies for the development and implementation of enterprise architectures. Enterprise architectures have played a large role in information technology and business process integration since OMB mandated their use to implement the intent of the Clinger-Cohen Act of 1996. As a whole, DHS and the rest of the federal government still have considerable work to do in this area. A federal enterprise architecture program management office (PMO) has been established to address the shortcomings across the agencies and departments.

[17] Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act), Public Law 104-106 Division E http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ090.pdf (accessed November 21, 2007) § 5125.

The lack of a mature DHS enterprise architecture was not attributable to the HSIN program management. With a well-developed enterprise architecture in place, the HSIN program management could have leveraged much of the information in the enterprise architecture to better define requirements, engage stakeholders, and plan implementation. The lack of a suitable enterprise architecture greatly impacted the program management's ability to build an efficient, non-duplicative system, but ramifications extend beyond the HSIN system. Relevant to homeland security information sharing, DHS must grasp the extent of the capabilities, interconnections, and data flows not only within its department but also within the federal government and the homeland security community to fully utilize data sources and build an information sharing enterprise.

Acquisition

Concurrent with the systems engineering and enterprise architecture struggles of the HSIN program were the growing pains DHS had with the lack of department wide policies and procedures for program management. These policies and procedures are used to manage the acquisition of complex systems. Acquiring HSIN in the absence of established policies is a recipe for disaster. With the urgency of satisfying DHS' mission needs, HSIN's accelerated schedule took precedence over employment of sound acquisition and program management practices. Developing a set of program management policies and procedures that can serve as a roadmap will serve to establish an environment of disciplined system acquisitions. Without this disciplined approach, other programs will be destined to repeat the mistakes of the HSIN program.

DHS has expended considerable effort to resolve its program management shortcomings with HSIN. Great strides have been made to correct the problems that

plagued HSIN in this area. A formal program management office was set up by the department to take a holistic approach to the management of the program. The HSIN Joint Program Office is addressing shortfalls in the system, focusing on stakeholder engagement. The HSIN program manager is also developing performance metrics to assess the system and its information sharing effectiveness.[18] One of the key problems with the program management of the HSIN program was the lack of involvement of the state and local users. They were not consulted on requirements or how the system would be used.[19] The new Joint Program Office has been set up to address this failure, employing a Stakeholder Relationship Management team to work closely with the system users. DHS, in several reports, has emphasized that the compressed deployment schedule was the reason for not engaging the users. Key tenets of program management emphasize the early and constant engagement of the users.

As discussed previously, the HSIN program was deficient in the planning phase of the program. The development and implementation of an enterprise architecture is an essential element of planning activity. Benefits of an enterprise architecture such as better defined requirements, user engagement, and implementation coordination were lacking with the expedited schedule of HSIN. For the Homeland Security Information Network, the transformation from islands of information to a distributed information system could have progressed to a more mature and useful state with an enterprise architecture in place.[20] Again, with the accelerated schedule and the immaturity of

---

[18] U.S. Department of Homeland Security, *Department of Homeland Security Fiscal Year 2007 Annual Financial Report*, http://www.dhs.gov/xlibrary/assets/cfo_afrfy2007.pdf (accessed November 25, 2007), 268.

[19] U.S. Department of Homeland Security, OIG-06-38, 13.

[20] U.S. Department of Homeland Security, OIG-06-38, 3-4.

processes and policies of a new executive department, HSIN was plagued by programmatic issues from its inception.

Legal Issues

Legal issues regarding the sharing of information have impacted the federal government for decades. The National Security Act of 1947 and additional reforms in the 1970's, following investigations of domestic surveillance during the Vietnam War, clearly established a divide between the Intelligence Community and law enforcement, specifically the Federal Bureau of Investigation (FBI).[21] As the government dealt with international banking fraud cases in the 1990's, there was a recognition of the need to have more cooperation between intelligence activities and law enforcement. The events of 9/11 brought all of these discussions to the forefront again. This time, however, Congress and the public were more willing to accept the compromises between security and privacy to ensure their safety. Two of the primary problems with legal implications are sharing information between the FBI and the Intelligence Community and sharing information between the federal government and state and local governments. Resolving each of these issues is crucial to making HSIN a viable, effective system for sharing homeland security information.

Federal

Prior to September 11, 2001, the FBI could not share information developed in a grand jury investigation or obtained through a court-authorized wiretap because of legal

[21] The Church Committee identified misuse of the domestic surveillance programs from the 1950's to the mid-1970's such as surveillance of American anti-Vietnam War protesters and civil rights leaders. The Foreign Intelligence Surveillance Act (FISA) of 1978, a form of oversight on the federal government's domestic surveillance programs, was a result of the Church Committee investigations. FISA and the Omnibus Crime Control Act of 1968 establish separate statutory frameworks for foreign intelligence and law enforcement interception of electronic communications, respectively.

prohibitions. This applied even if the information was related to terrorism. Section 203 of the USA PATRIOT Act changed this restriction.[22] The USA PATRIOT Act in Section 504 also permitted federal officers performing electronic surveillance under the Foreign Intelligence Surveillance Act to consult with federal, state, or local law enforcement personnel to coordinate their efforts against attacks by a foreign power. These changes were extraordinary to promote information sharing between law enforcement and the federal government.

To restrict the effects of these changes, Congress put sunset provisions on several sections of the USA PATRIOT Act, including section 203. Sunset provisions put an expiration date on certain sections of legislation and give Congress the opportunity to renew the provisions if they have been beneficial. In March 2006, President Bush signed the USA PATRIOT Improvement and Reauthorization Act of 2005, which repealed the sunset provisions. The legal changes made by the USA PATRIOT Act and the Homeland Security Act, which made the Department of Homeland Security responsible for sharing terrorism information among federal, state, and local government, were not trivial to implement. DHS had to identify all relevant providers and consumers of terrorism information, establish procedures for sharing information, and break down existing barriers, such as the barrier between the Intelligence Community and law enforcement. The sunset provisions may have had an impact on the deliberate progress made on the new information sharing procedures. The new laws put in place to facilitate

[22] "[I]t shall be lawful for foreign intelligence or counterintelligence… or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." USA PATRIOT Act of 2001, Public Law 107-56, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf (accessed November 19, 2007) §203.

information sharing have initiated many concerns regarding privacy and civil liberties. Privacy and civil liberties issues, such as the broader access to information by law enforcement and intelligence agencies as afforded by the USA PATRIOT Act, have had a direct impact on the HSIN implementation.

Privacy and Civil Liberties

Achieving the right balance between information sharing and privacy is a very difficult task. To balance the legal changes made in information sharing procedures, the Homeland Security Act put a privacy officer in the Department of Homeland Security to ensure that personal information was handled in compliance with the practices set out in the Privacy Act of 1974. The DHS Privacy Office conducts reviews on IT systems and data to determine if there is a privacy impact. A privacy impact assessment was conducted on HSIN in 2006. The assessment found that HSIN access to information is limited initially to activity-based reports. Sensitive information such as personal information is only shared with government or law enforcement HSIN users that have the appropriate clearance and a need to know. This meets the requirement of the USA PATRIOT Act, which allows access to information if it is in the performance of official duties. HSIN has been designed so that under no circumstances will personal information be shared with a private sector HSIN user.

On one occasion, the HSIN document library, which consisted of daily and periodic reports, was shut down because legal approvals had not been obtained to post the information. It took three months to obtain the approvals necessary to resume access to the document library.[23] On another occasion, the law enforcement community questioned whether HSIN was compliant with Title 28, Code of Federal Regulations, Part

[23] U.S. Department of Homeland Security, OIG-06-38, 15.

23, which regulates "multi-jurisdictional criminal intelligence systems… to safeguard the privacy and constitutional rights of individuals."[24] To maintain the system's utility through regulatory compliance, the HSIN program management worked to resolve this issue with the Department of Justice. The Department of Justice ruled that the HSIN system was compliant with Title 28, Code of Federal Regulations, Part 23.[25]

The Homeland Security Act also established an officer for civil rights and civil liberties to "review and assess information alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by employees and officials of the Department."[26] Despite the efforts of Congress to put oversight measures in place for privacy and civil liberties, several groups have expressed concerns about the expanded information sharing authorities and their privacy implications. The Electronic Frontier Foundation (EFF) responded to the USA PATRIOT Act by saying "The civil liberties of ordinary Americans have taken a tremendous blow with this law, especially the right to privacy in our online communications and activities."[27] Nancy Chang of the Center for Constitutional Rights echoed the sentiments of the EFF and others in her statement "[T]he Act sacrifices our political freedoms in the name of national security and upsets the democratic values that define our nation by consolidating vast new powers in the

[24] U.S. Department of Homeland Security, OIG-06-38, 23.

[25] U.S. Department of Homeland Security, OIG-06-38, 23.

[26] Homeland Security Act, § 705.

[27] Electronic Frontier Foundation, "EFF Analysis Of The Provisions of the USA PATRIOT Act," http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php (accessed November 25, 2007).

executive branch of the government."[28] Vigilance to comply with all regulations and laws is paramount to maintaining the trust of the system users and the American public. Without this trust, HSIN's relevance as a useful tool for the homeland security mission is questionable.

State

Federal information sharing initiatives were directed by the Homeland Security Act and the Intelligence Reform and Terrorism Prevention Act, which mandated an information sharing environment to share terrorism information nationwide. These statutory changes have helped at the federal level, but state laws remain a serious impediment to sharing across the entire homeland security community.[29] While the federal government can disseminate information to the state and local governments, state laws still have restrictions on state and local users disseminating information to the federal government. These restrictions will continue to limit HSIN's effectiveness if the homeland security community's frontline, the state and local governments, cannot disseminate information throughout the community. DHS must be cognizant of state laws as the implementation of HSIN continues. This awareness will ensure information sharing and privacy laws and regulations are adhered to as more state and local organizations get connectivity to HSIN.

---

[28] Nancy Chang, "The USA PATRIOT Act: What's So Patriotic About Trampling on the Bill of Rights?" In *Homeland Security and Terrorism: Readings and Interpretations*, ed. Russell D. Howard, James J. F. Forest, and Joanne C. Moore (New York: McGraw-Hill, 2006), 369.

[29] Under state laws similar to the federal Freedom of Information Act, the disclosure of various types of information to persons or government agencies may be exempted. The types include certain personal information, personnel records, some public records under court rules, and records whose disclosure would be "contrary to public interest" such as investigatory records. Maryland Attorney General, *Access to Government Records Under the Maryland Public Information Act*, http://www.oag.state.md.us/Opengov/whatisPIA.pdf (accessed March 30, 2008) 2.

All of the legislative reform that has facilitated better information sharing has been referred to as tearing down the wall.[30] This wall between law enforcement and the intelligence community has existed as a safeguard for American citizens and their individual rights. The federal government is very sensitive to this tenuous issue. In testimony to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence in 2002, General Michael Hayden,[31] Director of the Central Intelligence Agency, told the committee members "What I really need you to do is talk to your constituents and find out where the American people want that line between security and liberty to be."[32] This is an issue that everyone in the U.S. wrestles with more than six years after the events of 9/11. Congress plays a key role in the oversight of this delicate balance.

Congress must work to balance the need for information sharing with the preservation of individual rights. Laurence Tribe, a constitutional law expert, put the issue in perspective stating "civil liberties are not only about protecting us from our government. They are also about protecting our lives from terrorism."[33] Mr. Tribe acknowledges that increased government authority does not endanger civil liberties but is necessary to preserve them. This increased government authority strengthened the federal government. This change shifts authority from state and local governments to the

---

[30] U.S. Library of Congress, Congressional Research Service. *Sharing Law Enforcement and Intelligence Information: The Congressional Role*, by Richard A. Best Jr. CRS RL33873 (February 13, 2007) http://www.fas.org/sgp/crs/intel/RL33873.pdf (accessed August 4, 2007) 10.

[31] At the time of the testimony, General Hayden was the Director of the National Security Agency.

[32] U.S. Library of Congress, CRS RL33873, 15.

[33] Roger Dean Golden, "What Price Security? The USA PATRIOT Act and America's Balance Between Freedom and Security," In *Homeland Security and Terrorism: Readings and Interpretations*, ed. Russell D. Howard, James J. F. Forest, and Joanne C. Moore (New York: McGraw-Hill, 2006), 409.

federal government.[34] With this increased authority, the federal government must still be cognizant of state and local laws and regulations.

While the USA PATRIOT Act removed most of the barriers to sharing information between the Intelligence Community and law enforcement, longstanding procedures are still being overcome as DHS, FBI, and other federal agencies work through the new information sharing procedures that are being developed. DHS is still negotiating its place in the information sharing enterprise following IRTPA, which established the National Counterterrorism Center, the Office of the Director of National Intelligence, and the Information Sharing Environment (ISE).[35] Close coordination between the HSIN program management and the ISE program manager is necessary to ensure HSIN continues as a viable terrorism-related information sharing medium. Until responsibilities and procedures are resolved, HSIN's place in providing terrorism-related information to the federal, state, and local governments remains unclear. The sunset provisions in the USA PATRIOT Act that enabled improved information sharing also added uncertainty to the accessibility of information. The USA PATRIOT Improvement and Reauthorization Act of 2005 resolved much of the uncertainty but until the law was signed, there were delays in addressing the new information sharing authorities. Since there were no guarantees that the sunset provisions would be extended, the agencies

[34] Donald F. Kettl, *System Under Stress: Homeland Security and American Politics* (Washington D.C.: CQ Press, 2004), 93.

[35] Center for Strategic and International Studies, *Intelligence Reform and Terrorism Prevention Act of 2004*, http://www.csis.org/media/csis/pubs/041201_irtpa_overview.pdf (accessed August 4, 2007) 1.

involved moved very deliberately.[36] With the tremendous amount of change taking place, HSIN was not only implementing a new information sharing system but also new processes and procedures under which the system would operate.

Cultural Issues

The last area of impediments to the implementation of HSIN is cultural. These cultural impediments can be divided into three main groups: organizational culture differences between law enforcement and the Intelligence Community, organizational culture differences between the federal government and the state and local governments, and the transformation of disparate cultures into a new executive department – the Department of Homeland Security. In many respects, the cultural impediments are closely related to the programmatic and legal problems as cultural issues have manifested themselves within the programmatic and legal areas. For example, the inadequate planning on the HSIN program could also be attributed to the lack of established processes and procedures, which is typical of a new organization in transformation. DHS blamed the inadequate planning on the accelerated implementation schedule. The information sharing problems, while they predate the establishment of the Department of Homeland Security, are rooted in the mistrust and misunderstanding between the law enforcement community and external organizations. The wall between the Intelligence Community and law enforcement that acted as a legal safeguard is also a cultural

[36] Brian H. Hook, Margaret J. A. Peterlin, and Peter L. Welsh, "The USA PATRIOT Act and Information Sharing Between the Intelligence and Law Enforcement Communities," In *Homeland Security and Terrorism: Readings and Interpretations*, ed. Russell D. Howard, James J. F. Forest, and Joanne C. Moore (New York: McGraw-Hill, 2006), 394.

barrier.[37] The legal restrictions previously discussed reinforced the cultural differences between the Intelligence Community and the law enforcement community.

To address differences in organizational culture, the term organizational culture needs to be defined. Organizational culture is "a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."[38] These shared basic assumptions are exhibited in many ways, such as how the group communicates and makes decisions.

Law Enforcement - Intelligence Community Cultural Differences

As discussed in the last section on legal impediments, the cultural differences between law enforcement and the Intelligence Community have evolved since the late 1940's. The laws that created the wall between law enforcement and the Intelligence Community have created an environment that helped evolve the cultures into their current state. The basic mission of the FBI, specifically, and law enforcement, in general, is to apprehend and convict criminals. The law enforcement community develops information for the purpose of using it as evidence in criminal cases. Law enforcement's ultimate objective is the successful prosecution of a case. This objective explains why law enforcement officers protect this information so fervently. For the evidence to be admissible, it must be collected within legal guidelines. Prior to the USA PATRIOT Act,

---

[37] Devin Rollis, "The Wall Between National Security and Law Enforcement," in *Can't We All Get Along? Improving The Law Enforcement-Intelligence Community Relationship* (Washington, DC: NDIC Press, 2007), 143.

[38] Edgar H. Schein, *Organizational Culture and Leadership* (San Francisco: Jossey-Bass, 2004), 17.

this information could not be shared with the Intelligence Community. Even though there are exceptions, law enforcement is generally a reactive entity, responding to the commission of criminal acts. This culture of "protecting the case" and reacting to events has not been erased by the USA PATRIOT Act. While the FBI is a member of the Intelligence Community; the intelligence component of the FBI, which collects information on foreign intelligence activities, has a distinctly different culture and mission from the rest of the FBI.

The basic mission of the Intelligence Community is to develop information to inform consumers, whether it be national security policymakers or military commanders. Because the intelligence is derived from human sources, imagery, and/or interception of foreign communications; the sensitivity of the information requires protection of the sources and methods. To share the information, the recipient must have a "need to know." This restricted information sharing has evolved the idea that each agency of the Intelligence Community owns the information that they collect and analyze. Developing intelligence is more of an anticipatory, proactive activity, in contrast to law enforcement. The culture of the Intelligence Community wants to protect the sources and methods used to develop intelligence and restrict dissemination of intelligence to only those with a "need to know."

The lack of information sharing, called out in the Joint Inquiry and the 9/11 Commission, highlighted the cultural differences between the Intelligence Community and law enforcement. If an information sharing system like HSIN is to be effective, the cultural divide between the Intelligence Community and law enforcement must be bridged. The different cultures of law enforcement and the Intelligence Community,

which develop information into evidence and intelligence, respectively, must appreciate the common purpose that is afforded by statutory changes. The Director of National Intelligence, Mike McConnell, said the Intelligence Community needs to be guided by the mindset of "responsibility to provide" intelligence to national policymakers and military commanders within the bounds of protecting sources and methods.[39] Sharing critical information with all levels of government is critical to HSIN's success and the homeland security mission.

Federal Government - State and Local Government Cultural Differences

The American democracy is based in the principles of federalism—a system of government in which the state governments defer some powers to the federal government. The mission of homeland security can be traced back to the preamble of the Constitution, where the government is to "provide for the common defence."[40] It was recognized within the federal government that homeland security could not be strictly a federal government mission. The National Strategy for Homeland Security presented "legislative actions that would help enable our country to fight the war on terrorism more effectively." [41] The National Strategy for Homeland Security acknowledged the need to not overfederalize the homeland security mission. The National Strategy for Homeland Security recognized that "[o]ur structure of overlapping federal, state, and local governance… provides unique opportunity and challenges for our homeland security

[39] Mike McConnell, "Overhauling Intelligence," *Foreign Affairs* 86, no. 4 (July/August 2007), under "Culture Shock," http://www.foreignaffairs.org/20070701faessay86404/mike-mcconnell/overhauling-intelligence.html (accessed December 8, 2007).

[40] U.S. Constitution, preamble.

[41] President, *National Strategy for Homeland Security*, x.

efforts."[42] The opportunity comes from the expertise and commitment of local agencies and organizations involved in homeland security. State and local governments have critical roles to play in homeland security. The challenges, however, present real impediments to an effective homeland security enterprise. These challenges are built around the cultural differences that have developed as a result of our system of federalism. DHS was set up in the federal government to coordinate homeland security efforts throughout the nation. The day-to-day work on the ground, however, is done by the state and local governments. These different perspectives cause friction.

DHS must resist the urge to make all homeland security initiatives and responses a federal effort. In the Dark Winter exercise[43] in 2001, former Oklahoma Governor Frank Keating, a participant in the exercise, noted that "the federal government all too often acts like a 500-pound gorilla."[44] Governor Keating acknowledged that many components of a national response to terrorism must be federal but "that the response to terrorism does not begin and end in Washington. Trust local governments, local agencies, and local citizens to do the right thing, because in the end, they are the real targets of terrorism."[45] There are capabilities and authorities that each level of government possesses that must be used in concert with the other government organizations' strengths to execute the homeland security mission. Coordination among

---

[42] President, *National Strategy for Homeland Security*, vii.

[43] Dark Winter was an exercise to evaluate the national response to the use of a biological weapon on the American populace.

[44] Frank Keating, "Catastrophic Terrorism: Local Response to a National Threat" In *Homeland Security and Terrorism: Readings and Interpretations*, ed. Russell D. Howard, James J. F. Forest, and Joanne C. Moore (New York: McGraw-Hill, 2006), 264.

[45] Keating, 264-265.

all levels of government can turn the challenges into opportunities and create more positive perceptions among the homeland security community.

Distrust of the federal government, fiscal constraints, and dissimilar missions are manifestations in the state and local governments of the different cultures. The personnel and expertise that provide the tactical information come at a great cost to state and local governments. These new missions that help protect the citizens of each jurisdiction require funding. Local governments must increase their budgets or reduce other services if they are to address the homeland security mission. Federal grants have helped as a temporary measure but the contrast between the fiscal austerity of the state and local governments and the affluence of the federal government is difficult to ignore. The lack of communication between DHS and the state homeland security organizations has exacerbated the distrust of the federal government. The DHS Inspector General report on HSIN in 2006 cited that no feedback is provided to state and local governments on information that is sent to DHS and that states were not consulted on the rollout of HSIN to the county level.[46] The latitude given to the states to develop homeland security organizations has also hampered communications. In some states, homeland security organizations are an independent cabinet department dedicated to homeland security while in other states; homeland security organizations are a division of a larger cabinet department such as public safety, emergency management, or law enforcement.[47] Numerous approaches for establishing homeland security organizations across the country make processes and procedures more complicated for DHS. The different

---

[46] U.S. Department of Homeland Security, OIG-06-38, 15.

[47] National Governors Association Center for Best Practices, *2006 State Homeland Security Directors Survey*, http://www.nga.org/Files/pdf/0703GOVGUIDEHS.PDF (accessed September 3, 2007) 3-4.

perspectives between the local governments and their first responders and DHS and its administrators perpetuate the cultural differences.

Through their frequent interactions and proximity, most citizens' closest relationship with government is at the local level. This close relationship builds trust between the people and the state and local governments. Without the citizens' trust, state and local governments will not contribute information to HSIN. Whether it is concern about jeopardizing a criminal case or the belief that homeland security is federally-focused; federal, state, and local governments must engage and communicate to develop an understanding of each other's cultures. The state and local governments as well as local law enforcement must build a culture of information sharing since the data provided locally is an important source of information for the federal and state governments. Local law enforcement and governments also benefit from receiving actionable information from the federal and state governments for use within their local jurisdictions.

DHS Transformation

The establishment of the Department of Homeland Security is the most extensive reorganization in the federal government in over 50 years. As DHS transforms itself from 22 separate agencies into an integrated executive department, it must deal with the existing cultures brought by each agency. These diverse cultures range from the Coast Guard, a uniformed military service, to the Secret Service, which provides protective services and conducts criminal investigations, to the Federal Emergency Management Agency, which supports the nation with emergency preparedness and response. All of the department's agencies have diverse missions but with the common thread of

homeland security. With the varied mission and dynamic priorities, the different cultures of each component agency are reinforced with the often independent missions that each agency performs. Each agency has its own responsibilities and issues that it addresses using the accepted norms, values, and beliefs that worked before DHS was formed. Trying to build a "homeland security" culture with each agency working its own mission will be extremely difficult. With these separate cultures, work must be done to build the practice of information sharing not only within the department but also within the homeland security community. If DHS does not embrace a culture that values information sharing and the benefits of HSIN, it is unlikely that external organizations will adopt the system as their homeland security information sharing medium. DHS must create an environment that fosters the creation of a common, overarching homeland security culture. In a subsequent chapter, this paper will make several recommendations that will facilitate the development of this common homeland security culture.

The majority of effort spent on salvaging the Homeland Security Information Network has been devoted to correcting programmatic and legal issues. Numerous measures have been employed to improve the effectiveness of HSIN – the creation of a program management office to address all aspects of the HSIN implementation, the ongoing development of a departmental enterprise architecture, and developing information sharing procedures within legal guidelines. In a broad scope, Congress has enacted new laws such as the USA PATRIOT Act, the Homeland Security Act, and the Intelligence Reform and Terrorism Prevention Act to enable better information sharing throughout all levels of government. HSIN is leveraging these statutory changes. Despite its problems, the department remains committed to its mission of homeland

security information sharing and to resolving HSIN's problems. Charles Allen, DHS Chief Intelligence Officer, recently said "as the system has and continues to mature, the Department remains committed to improve its usefulness and accessibility."[48]

Cultural issues are usually mentioned in association with HSIN's programmatic issues but only as a placeholder. These cultural issues have not been worked as aggressively as other issues such as implementing an enterprise architecture or putting metrics in place to measure system performance improvements. Without taking a more aggressive approach to resolving the cultural barriers affecting information sharing, these barriers will remain in place, reducing HSIN's effectiveness in the homeland security mission. Cultural changes that will effect positive impacts on information sharing have a much longer timeline than gathering user requirements or developing an enterprise architecture. The cultures that exist in law enforcement, state and local governments, the Intelligence Community, and within DHS weren't created in months. These cultures have evolved over the course of many years, through many formative events. Certainly the legal and programmatic issues of HSIN need to be fixed, but without implementing measures that will change the culture of the homeland security community, HSIN will be burdened with the same baggage that has affected information sharing for decades. The remaining chapters of this paper will address what drives these cultures and how the cultures can be changed to build an overarching homeland security culture, where each agency in each level of government feels a responsibility to its constituents to use and share homeland security information to provide benefit to all.

---

[48] House Committee on Homeland Security, *The Homeland Security Information Network: An Update on DHS Information-Sharing Efforts*: Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security. 109th Cong., 2d sess., September 13, 2006, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:35623.pdf (accessed September 2, 2007) 13.

IV. Culture

As defined in the previous chapter, organizational culture is "a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."[1] This pattern of shared basic assumptions serves many purposes in an organization. It creates boundaries that define differences between organizations. These differences build a sense of identity for the members of an organization. This sense of identity fosters commitment to the organization. The individual member is no longer concerned only with his self-interest, but on the good of the organization. The sense of identity and belonging in an organization's members develops stability. Each of the members knows what the accepted norms and values are for their organization. They know what is expected of them. This allows members to quantify what is distinctive about their organization.

Organizational Culture

In the study of organizational cultures, cultures are often described as having multiple levels. The most visible level of culture is composed of artifacts: an organization's behavior patterns, language, and organizational structure and processes.[2] This behavioral component of organizational culture is how the organization does things. These are the behavior patterns that new employees are encouraged to follow when they

[1] Schein, 17.

[2] Schein, 25-26.

join an organization.[3] While this is the most visible level of culture, it is the most difficult level to interpret but also the easiest to change. At an intermediate level, culture is represented by values and beliefs shared by the group. These values and beliefs are learned from experiences with the organization. If these experiences are perceived as successes, the values and beliefs become more ingrained in the culture. The organization's values and beliefs are on a conscious level that can be articulated as the basis for guiding behavior and reacting to situations.[4] With continued success, the organization's values and beliefs transform into an organizational philosophy. Often, certain behaviors are unexplained by the espoused values and beliefs of an organization. This leads to the next level of culture to explain these behaviors. At the deepest and least visible level, culture refers to the assumptions shared by the group. The term assumptions is used because these beliefs are taken for granted and are considered nonnegotiable by the group.[5] This level of culture is the most difficult to observe and change. These assumptions, shared by the group, are not open to discussion. The stability desired by the members of organizations and driven by shared assumptions make it difficult to change organizational cultures. These assumptions endure even when members of the group change. These assumptions are the source of the group's behavior and values.

Each level of culture influences the other. It is natural to assume that a group's behavior would be influenced by its shared values and assumptions. These values and

---

[3] John P. Kotter and James L. Heskett, *Corporate Culture and Performance* (New York: The Free Press,1992), 4.

[4] Schein, 29.

[5] Schein, 25.

assumptions are the unwavering guidance for the organization. Acting outside of the behavioral norms is inconceivable for the organization's members. The shared values and assumptions of an organization's culture are deeply rooted. A group's behavior and processes can also influence the group's values and assumptions. If a stimulus such as the modification of the organizational structure changes behavior or processes, this may challenge and, ultimately, change the organization's shared values and assumptions. This idea will be important as methods to change an organization's culture are discussed later.

Types of Culture

Types of organizational cultures have been frequently studied in relation to corporate performance. These culture types are equally relevant for government organizations and their performance. While government organizations are not concerned with making a profit, government organizations are concerned with how effectively they are performing their mission. Organizational cultures have been classified in a number of ways by researchers. The three types of organizational cultures that are most relevant to the homeland security community are role, task, and power.[6]

The first type of organizational culture that is useful in understanding the homeland security community cultural differences is the role culture. In a role culture, employees may get very little feedback on their performance. This is because role cultures develop in industries where financial stakes are low such as financial-service organizations and large portions of the government.[7] In an industry with many rules and

---

[6] Roger Harrison, "Understanding Your Organization's Character," *Harvard Business Review* 50, no. 3 (May/June 1972): 121.

[7] Terrence E. Deal and Allan A. Kennedy, *Corporate Cultures: The Rites and Rituals of Corporate Life* (Reading, MA: Addison-Wesley Publishing Co., 1982), 119. In *Corporate Cultures*, the role culture is referred to as the "process culture." The term "role culture" will be used in this paper for consistency.

regulations and little feedback, organizations become very focused on how they do things, not on what they do. A role culture places great emphasis on formal procedures. While a role culture may be harmful to performance in a fast-paced business environment, citizens need to be able to depend on the government for critical services and on financial-service companies for solvency when they need their money.[8] Risk-taking is not part of the role culture. This type of culture can be very bureaucratic but is also very predictable. Organizations with a role culture normally have a well-defined hierarchical structure.

Another type of organizational culture is the task culture. Task requirements dictate the way work is completed in a task culture. In a task culture, its members enjoy the most autonomy of the culture types discussed. This freedom gives the members flexibility in how they perform their work. This flexibility builds a strong belief in the organization's culture, which in return builds a unity of purpose. Employees in a task culture are generally satisfied with and committed to their organization.[9] There is a high level of teamwork among members of a task culture because of the common purpose that exists. Members from within the organization are brought together to form teams to solve a particular problem. Individual expertise is leveraged in this team construct.[10]

A third type of culture is the power culture. A power culture typically has a centralization of power whether it be a strong leader or a central headquarters. This centralization of power and minimal bureaucracy allows a power culture to react quickly

---

[8] Deal and Kennedy, 120.

[9] Susan Cartwright and Cary L. Cooper, "The Role of Culture Compatibility in Successful Organizational Marriage," *Academy of Management Executive* 7, no. 2 (May 1993): 62.

[10] Harrison, 122.

and decisively to a changing situation. In power cultures, employees have the least autonomy of the three culture types discussed. Employees are expected to follow instructions without question. Employees are seldom involved in decision-making in a power culture. This is because of the high level of constraint imposed by the power culture. The employees' commitment to the organization in a power culture is typically based on compliance rather than loyalty.[11] Some loyalty may develop based on the success of the organization.

An important characteristic of organizational culture is the ability to adapt. The environment in which an organization operates determines what things the organization values as it seeks success. Therefore, the environment has a great influence in shaping the organization's culture.[12] Adaptive cultures "help organizations anticipate and adapt to environmental change" with the goal of increasing organizational performance over the long term.[13] In the public sector, cultures are shaped by myriad of rules and regulations. This often results in a culture characterized by a priority on how things are done with less emphasis on results. Adaptive cultures have been described as "a risk-taking, trusting, and proactive approach to organizational [life] … There is widespread enthusiasm, a spirit of doing whatever it takes to achieve organizational success. The members are receptive to change and innovation."[14] A key point about adaptive cultures is that they do not change merely to change. The change associated with adaptive

---

[11] Cartwright and Cooper, 62-63.

[12] Deal and Kennedy, 13.

[13] Kotter and Heskett, 44.

[14] Ralph H. Kilmann, "Five Steps for Closing Culture-Gaps," in *Gaining Control of the Corporate Culture,* ed. Ralph H. Kilmann, Mary J. Saxton, and Roy Serpa (San Francisco: Jossey-Bass Publishers,1985), 356.

cultures is constructive. The change may be in response to validated customers' needs, a new business opportunity, or an innovative new way of doing business. It is acceptable in an adaptive culture to initiate change to help the organization sustain its performance. Non-adaptive cultures tend to be bureaucratic, reactive, and risk averse. Because of these characteristics, the non-adaptive culture does not change quickly to adapt to its environment. The financial services industry including banks and insurance companies is a good example of a non-adaptive culture. The industry's reaction to an external change is usually measured and deliberate. This risk-averse approach is good for the customer and his money.[15]

Another important characteristic of organizational culture is the strength of culture. A strong culture is defined as shared values and assumptions that are "intensely held and widely shared."[16] Strong culture in an organization is built not only by a strong commitment to the organization's shared values and assumptions but also by the large number of members. The more members within an organization that believe in those shared values and assumptions, the stronger the culture is. A strong culture intensifies the influence of culture on an organization's behavior and cohesion. A strong culture provides well-established rules and norms for behavior. The strong culture builds a unity of purpose within the organization because of the members' commitment.[17] Strong cultures can be very powerful when a group needs to take a coordinated action. The unity of purpose in a strong culture gives clear guidance to the organization on how it

---

[15] Deal and Kennedy, 148-149.

[16] Stephen P. Robbins, *Organizational Behavior: Concepts, Controversies, Applications*, 8th ed. (Upper Saddle River, NJ: Prentice Hall, 1998), 598.

[17] Robbins, 598.

responses to a situation. Because of the strong commitment to the values and assumptions of the organizational culture, a strong culture tends to be very stable over time. The antithesis of a strong culture, a weak culture, is typified by less commitment to the organization's shared values and assumptions. This may result in differing shared values and assumptions across the organization. Therefore, the weak culture has less influence across the organization. Without the guidance that a strong culture provides, organizations with weak cultures are unsure how to respond to their environments.

Organizational cultures are usually referred to as a single entity. This may be true in a small organization but in a larger organization, especially one that is geographically dispersed or performs various functions; there will be sub-cultures associated with each location or each function performed. Culture is group-based. As each geographically separated group performs their tasks, a somewhat different culture may form. The location-based subcultures form because of different environments, interactions, and local group leadership.[18] Groups that perform different functions may have different cultures as well. Often the set of values and assumptions that define different occupations are developed in the course of their professional training. Subcultures will develop with groups because they are more suited to the function that the group performs.[19] For example, one would expect the finance department of an organization to have a role subculture, which is risk averse and process oriented. The corporate or organizational culture is really the set of values and assumptions shared by all of the organization's members. Different subsets of the organization may have their own

[18] Robbins, 597.

[19] Schein, 275.

shared values and assumptions based on their location or their occupation.[20] In a strong culture, subcultures provide healthy tension among groups. In a weak culture, a strong commitment to an organizational set of values and assumptions is lacking. Therefore, individual subcultures may clash with the organization's culture and attempt to guide behavior outside its group. If one group has a role culture and tries to impose this on another group that typically operates in risk-taking culture; the company may lose its cultural guidance.[21] This undermines the stability sought by organizations.

A strong organizational culture is not necessarily good or bad. If an environment is stable, a strong, non-adaptive culture will be sufficient to maintain effective organizational performance. This strong culture is an asset in a stable environment. The consistency of behavior and processes associated with a strong culture will benefit the organization. Organizational culture tends to be stable over time but if the environment changes, the way things are done may need to change as well. This is where a non-adaptive culture breaks down. An adaptive culture is key to addressing change. If the values and assumptions cannot adapt to changes in the organization's environment to maintain organizational effectiveness, then the organization's culture is a liability.[22] The cultural artifacts such as behavior and processes may lead to diminished performance and ultimately failure if they don't match up with the new environment. A dynamic environment will be a challenge to the organization with a non-adaptive culture. A strong culture can maintain good organizational performance if the culture has values and assumptions that support adaptability. Organizations must be able to adapt to a changing

---

[20] Robbins, 596.

[21] Deal and Kennedy, 152.

[22] Robbins, 602.

environment.[23] In a dynamic environment, the most important aspect of culture is the ability to adapt to change.

Collision of Cultures

Both the law enforcement community and the Intelligence Community are examples of strong cultures, characterized by a strong commitment to each community's values and commitments. Following the events of 9/11, these two communities have found it necessary to work closely together, exchanging information and ideas. Each community has its own process for handling information. Brent Scowcroft, former National Security Advisor, describes the cultural differences between law enforcement and intelligence personnel as:

> law enforcement personnel start with an incident, which they investigate with the goal of bringing the people responsible to justice. Therefore, law enforcement personnel have a hard time sharing information because they must protect the evidence and documentation of the investigation. On the other hand… intelligence personnel begin with a flood of material, looking for patterns to find indications of the incident before it happens. Therefore they must share information to compare ideas.[24]

Law enforcement and the Intelligence Community have operated like this for decades. Their collaboration and sharing information is complicated by their two distinct cultures. The Intelligence Community can be categorized as a role culture. In the execution of their work, they are focused on the process of sifting through information to find the patterns. The law enforcement community is also driven by processes and procedures but also is focused on the task. Each case is different so how they function is based on the

---

[23] Kotter and Heskett, 142.

[24] Devlin Kostal, "British Military Intelligence-Law Enforcement Integration in the Irish War of Independence, 1919-1921," in *Can't We All Get Along? Improving The Law Enforcement-Intelligence Community Relationship* (Washington, DC: NDIC Press, 2007), 138.

situation. This is representative of a task culture. In the context of corporate mergers, the combination of a role culture and a task culture could be problematic.[25] While the interaction of law enforcement and the Intelligence Community does not represent a corporate merger, the problems of different culture types are evident. A role culture's bureaucracy may be overwhelming for a task culture, which is accustomed to having autonomy to complete its work. On numerous occasions, law enforcement has been vocal about the "need to know" and overclassification of information by the Intelligence Community. This stems from the rules and procedures in place to govern the process of classifying and disseminating information.

The federal government often acts as the strong headquarters in a power culture in its interactions with state and local entities, dictating what programs will be implemented and how. There is a tendency for the federal government to establish programs that are federal-centric. With a focus at the federal level, plans are sometimes not executable at the state and local levels. The Homeland Security Advisory Council's Homeland Security Culture Task Force observed that DHS must move away from this model.[26] Public welfare including homeland security is the responsibility of the individual states. The states' ability to fund homeland security programs is often limited.[27] DHS controls the majority of the homeland security funding and has the responsibility to coordinate the national effort required to secure the homeland yet, the local and state governments have the manpower needed to effect the DHS programs. The combination of a power culture

---

[25] Cartwright and Cooper, 67.

[26] U.S. Department of Homeland Security, Homeland Security Advisory Council, *Report of the Culture Task Force, January 2007*, http://www.dhs.gov/xlibrary/assets/hsac-culture-010107.pdf (accessed September 1, 2007), 6.

[27] Saxon Graham, *American Culture: An Analysis of Its Development and Present Characteristics* (New York: Harper & Brothers, 1957), 321.

and any other type of culture most likely will have negative results. The loss of autonomy for the non-power culture and the extreme cultural differences make the working relationship difficult. A cooperative, collaborative relationship is required. DHS has begun to appreciate the importance of the non-federal HSIN users as it works to engage users to make HSIN a usable, effective information sharing system.

The establishment of DHS exemplifies the problems faced when there are many subcultures in an organization without a strong culture. The cultures of each agency in DHS have developed over decades based on the functions performed in the agency. As a federal department, DHS has adopted an "all hazards" focus while its component agencies focus on law enforcement, disaster response, and intelligence analysis among its myriad functions. Building a new executive department that has a high priority mission is a massive undertaking. Trying to build a department-wide culture in an environment with so many strong subcultures is equally challenging. These subcultures introduce friction into the relationships before organizational agendas and histories are added to the situation. This situation also provides tremendous opportunities as the different agencies can learn from each other's culture. The subcultures have been valuable to each agency in their past successes. The strengths of the individual subcultures must be cultivated but not at the expense of the organization. DHS must find a way to leverage the different subcultures to build a culture greater than the sum of its parts. Building this department-wide culture requires commitment from leadership and the employees to maintain the lengthy process. Through training, incentives, and more interaction among component agencies, DHS and its employees can effect the change needed to transform the

department. Recommendations for methods to build this new culture are discussed in the next chapter.

Lack of Trust

There is a fundamental gap that cuts across the three areas of cultural differences affecting HSIN. That gap is a lack of trust among the organizations in the homeland security community. This lack of trust comes from not knowing what to expect from the other organizations. Within a culture, there is a fundamental trait that is required to be effective, trust. With an absence of trust is the absence of stability and shared commitment necessary to be a functioning culture. A lack of trust is pervasive across each of the three areas of culture differences. By understanding the cultures of the other organizations in the homeland security community, members know what guides the behaviors of the other organizations.

As a part of their culture, people in a group are taught loyalty to their group. This loyalty is built through the sense of identity that comes with belonging to a group. Because of their differences, people outside the group are often distrusted. Trust can be created but it takes time. Trust will develop with frequent interaction between groups. This interaction could range from periodic meetings to collaboration on a project. Contact and interaction reduce mistrust as groups develop an understanding of the other groups' behaviors, beliefs, and assumptions, i.e. their culture. With the vast differences of culture in the homeland security community, it is not unexpected that trust would be lacking among the community members. The initial degree of trust among individuals

and between organizations may be based on relationships, such as superior to subordinate and peer to peer, or stereotypes based on individual or organization function.[28]

Prior to the events of 9/11, the interaction between law enforcement and the Intelligence Community was virtually nonexistent. Their interaction was well documented as separation by a wall. The legal barriers were removed by the USA PATRIOT Act but decades of stereotypes and misperceptions have been slow to change. There was no Department of Homeland Security prior to 2002. State homeland security offices did not exist either. Establishing relationships with state homeland security offices in a high threat environment has also been slow and cumbersome as state and federal agencies develop procedures and interpret legal authorities and responsibilities. DHS was established as an executive department as a direct result of the terrorist attacks on the U.S. Its history is short compared to many of its component agencies that have functioned as standalone entities for decades. Each of these agencies had limited interaction outside of its core function area. It is clear why trust is not yet where it should be. Each of these organizations has been cast into unfamiliar territory, working with unfamiliar partners.

This lack of trust reaches beyond a personal or organizational level. It is also present at the system level as some law enforcement personnel have not used HSIN because they did not trust HSIN to protect law enforcement information that they place on the system. Law enforcement personnel have continued to rely on trusted personal contacts within the law enforcement community instead of depending on HSIN. The trust that exists within the law enforcement community must be built and maintained

---

[28] David S. Alberts and Richard E. Hayes, *Understanding Command and Control* (Washington, DC: CCRP Publication Series, 2006), 44.

among all homeland security organizations to make homeland security information sharing effective using HSIN as the information sharing system. After seeing the success of a six month pilot effort to develop a Community of Interest on HSIN for intelligence professionals, First Sergeant Lee Miller of the Virginia State Police said "This community has created trusted relationships that ultimately is a more powerful tool than any network or portal and these relationships will remove the resistance to sharing information that has plagued government response in the past."[29]

HSIN's Biggest Impediment

The cultures that exist in law enforcement, state and local governments, the Intelligence Community, and within DHS represent some very strong cultures that have evolved over several decades, if not longer. There is strong commitment to the shared values and assumptions within each organization. The events of 9/11 and the subsequent change in the national security situation represent a big change to each organization's environment. This environmental change requires changes in each level of culture for each organization in the homeland security community to continue to perform in an effective manner. Each of these organizations now has more interdependent relationships than before 9/11 with the other homeland security community members. The organizations require a mutual change in culture to embrace the need to collaborate and share information.

HSIN, which was created as a tool to improve information sharing, has seen renewed efforts to resolve problems with its implementation. Subsequent to the

[29] House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Fixing the Homeland Security Information Network: Finding the Way Forward For Better Information Sharing*, 110th Cong., 1st sess., May 10, 2007, http://homeland.house.gov/SiteDocuments/20070510132259-40476.pdf (accessed November 30, 2007).

appointment of Charles Allen as DHS Assistant Secretary for Information Analysis and Chief Intelligence Officer,[30] efforts were increased to engage HSIN stakeholders. A program management office was set up to specifically resolve user problems with HSIN. The Homeland Security Act of 2002 laid the legal foundation for HSIN to share homeland security information. The Intelligence Reform and Terrorism Prevention Act of 2004 established a program management office for the Information Sharing Environment to improve information sharing in a broader context. These legal and programmatic areas have been areas where the federal government and DHS have focused their attention. Each of these legal and programmatic issues are non-trivial but represent issues that can be resolved with the application of resources and in a reasonable timeframe.

In a DHS Inspector General report in 2006, it was stated that "DHS officials anticipated when they first released HSIN that culture might become an issue, but they did not have time or resources to build the trusted relationships necessary to overcome this issue."[31] For the department to dismiss the cultural aspect of HSIN's implementation, even in a resource- or schedule-constrained environment, shows the gravity of HSIN's problems.

Changing culture does not happen overnight. A 1993 GAO report on organizational culture stated "that a culture change is a long-term effort that takes at least

[30] Mr. Allen's position was elevated to Under Secretary for Intelligence and Analysis by Public Law 110-53 on August 3, 2007.

[31] U.S. Department of Homeland Security, OIG-06-38. 33-34.

5 to 10 years to complete."[32] The cultural dimension of HSIN should have been addressed in parallel with the programmatic and legal issues. While a new culture would still not be fully developed at this time, at least, the new culture would be several years closer to maturity. Understanding that changing culture is a long term process may not be obvious to everyone. Each organization and its leadership must give the process of cultural change time to evolve. DHS needs to build those trusted relationships to overcome mistrust, bureaucracy, and internal subcultures, which stymie the use of HSIN. The cultural dimension was present at the HSIN program inception and still remains the largest impediment to HSIN's ultimate success. Cultural differences will never be completely removed across the homeland security community because these cultures have developed from the tasks and missions of each respective organization. The key is to find common ground on which these organizations can build trust and establish a unity of effort. The common ground is the shared responsibility to prevent and reduce vulnerability to terrorism in the United States.

To build these trusted relationships and test the procedures put in place by DHS, various homeland security organizations conduct periodic exercises. In 2007, the U.S. Joint Forces Command conducted an exercise, Noble Resolve, in conjunction with the U.S. Northern Command, DHS, and several states, giving the participants a chance to work with people and ideas that they may not normally work with. In the exercise's terrorist scenario, the Virginia Fusion Center worked with state officials and exercise

[32] U.S. General Accounting Office, *Organizational Culture: Techniques Companies Use to Perpetuate or Change Beliefs and Values*, GAO/NSIAD-92-105. http://archive.gao.gov/d31t10/146086.pdf (accessed August 11, 2007), 2.

participants to assess information sharing in the homeland security community.[33] Exercises like Noble Resolve build relationships and improve vital information sharing capabilities across federal, state, and local governments.

[33] U.S. Joint Forces Command, "Noble Resolve 07-1 yields new opportunities for experimentation," http://www.jfcom.mil/newslink/storyarchive/2007/pa053107.html (accessed March 30, 2008).

V. Recommendations

After discussing some of the different types of cultures that are represented in the homeland security community and identifying several of the cultural differences that impact HSIN, the next logical step is to discuss how to resolve these cultural differences. One of the obvious ways is to change cultures across the homeland security community. This would be a massive undertaking. The Homeland Security Advisory Council's Homeland Security Culture Task Force recommended a more meaningful approach. Their recommendation was to create an "overarching/blended… diverse but mission focused Homeland Security culture."[1] While the task force's recommendation was aimed at DHS, the recommendation is equally appropriate for the diverse homeland security community as a whole. An overarching, mission-focused culture would be ideal for homeland security, which has always been a national effort even though many have seen it as a federal effort. The key is to find common ground on which these organizations can build trust and establish a unity of effort. The common ground is a shared responsibility to prevent terrorism, which is the key threat to the homeland.

Cultural differences can never be completely removed across the homeland security community because these cultures have developed from the tasks and missions of each respective organization. This overarching culture would not destroy the unique cultures that have developed over many years but would enhance each organization's contribution to the homeland security mission. With this blended culture in place, information sharing would be the new norm. HSIN would be the key tool to enable and enhance information sharing.

---

[1] U.S. Department of Homeland Security, "Report of the Culture Task Force," 5.

Techniques to Change Culture

How does this cultural change begin? As discussed earlier, the deeper levels of culture affect behavior but behavior can also affect and, ultimately, change an organization's values and assumptions. Since behaviors are easier to change, that should be the level of culture where the change begins. There are various techniques that are effective in changing culture. Strong leadership is one of the most important and effective ways to change an organizational culture. Leaders usually have well-developed ideas of how the organization should do things and the organization's role in its environment. These ideas will be articulated by leadership to the organization, both directly and indirectly through their behavior. Their behavior provides clues as to what is expected from the members of the organization. The initial culture change may result from processes and behaviors that were impacted by the leader's articulated values and assumptions implemented in the organization. With organizational successes, these changes begin to be adopted by the organization. Leaders communicate their values and assumptions by putting emphasis on particular topics. Members of the organization pay attention to these cues and adjust their behaviors accordingly. Therefore, the leaders of an organization play a large role in the change and management of culture.

DHS recognized the need for strong leadership to effect changes on the HSIN program and their intelligence organization in general. In August 2005, Charles E. Allen was appointed Assistant Secretary of Homeland Security for Information Analysis and DHS Chief Intelligence Officer. In these roles, he leads and manages the DHS intelligence enterprise. Allen has leveraged his extensive experience in the Intelligence Community to build an organization that can work across the local, state, and federal

levels as well as with the Intelligence Community and law enforcement. From his early days as Assistant Secretary for Information Analysis and Chief Intelligence Officer, Allen has placed great emphasis on correcting the problems of the HSIN program. Allen saw the importance of providing a viable means to exchange information with homeland security partners at the local, state, and federal levels. Allen also recognized the importance of HSIN as a tool to facilitate information sharing, which is essential to building the DHS intelligence enterprise.

Another way to change organizational culture is through training. This training may be communicating the benefits of a new process that is aimed at making cultural change or it could be teaching the organization new skills to cope with a changing environment. Regardless, this training creates a common ground where members of the organization can discuss and work through the change. The training may establish a common language for the organization to resolve a lack of understanding. Charles Allen, DHS Chief Intelligence Officer, has instituted intelligence analyst training to enhance the DHS employees' analytic skills. DHS also intends to offer this training at the state and local levels. This training not only builds skill levels for other organizations but establishes a common vernacular so analysts can collaborate better with their peers. By speaking a common language and understanding how intelligence is developed and utilized, there will be an improved understanding of the information needs of HSIN users at the federal, state, and local levels. Equipped with a set of common skills and a better understanding of their peers, trust will be built among the analysts who may have different values and assumptions but now have a common function. Trust will close the gap of cultural differences. What may have started with the goal of developing better

intelligence analysts could evolve into more trust, changing cultures, and utilizing HSIN as the primary information sharing tool in the homeland security community. At a higher level, the Information Sharing Environment implementation plan recommends training based on applicable laws, regulations, and policies. This training will familiarize employees with the Information Sharing Environment, the legal basis for information sharing, efforts to work with state and local governments, and to promote an information sharing culture.[2]

Because collaboration and cooperation are such a key part of homeland security information sharing and HSIN's effectiveness, these behaviors must be rewarded. Incentives and rewards show the employees what is important to the organization. Incentives and rewards are another method of changing culture. These incentives and rewards reinforce the behaviors needed to change the culture to a more collaborative, cooperative setting. These incentives will encourage people to find new ways of doing things. Individual behavior and performance remain important but reinforcing cooperative behavior within and between organizations is vital to building trust and collaboration. For HSIN to be an effective information sharing system, collaboration must be the norm. Through its role as a conduit for information sharing, HSIN will reinforce the collaboration. In the Information Sharing Environment implementation plan, incentives are mentioned as one of the factors upon which the success of an overarching information sharing culture is dependent. These incentives range from the

[2] Office of the Director of National Intelligence, Office of the Program Manager-Information Sharing Environment, *Information Sharing Environment Implementation Plan*, http://www.ise.gov/docs/reports/ise-impplan-200611.pdf (accessed February 9, 2008), 85.

individual to the agency and department level, rewarding improvements in information sharing practices and information sharing accomplishments.[3]

Intelligence Fusion Centers

The most significant technique to effect cultural change is to place personnel from one organization within other homeland security community organizations. Since these personnel are still members of their parent organization, they would not give up their existing values and assumptions but would experience the other organization's culture to gain a better appreciation for how that organization operates and why. Anthropologists use the term, acculturation, to describe the "process of change that takes place when two different cultures come into direct contact."[4] Acculturation results from the contact, conflict, and adaptation of the two different cultures. The integration mode of acculturation "leads to some degree of change in both groups' cultures and practices."[5] Ideally, the change in both cultures incorporates the best of each culture. An equally important benefit of this exchange of personnel is the sharing of expertise among the homeland security community organizations. One Intelligence Community official referred to this exchange of personnel as an "exchange of hostages."[6] In an environment of distrust, sending a valued employee to an organization that is not well understood or trusted is counterintuitive. Optimistically, however, this exchange of personnel yields

---

[3] Office of the Director of National Intelligence, *Information Sharing Environment Implementation Plan*, 84.

[4] Marjorie H. McEntire and Joseph C. Bentley, "When Rivals Become Partners: Acculturation in a Newly-Merged Organization," *International Journal of Organizational Analysis* 4, no. 2 (April 1996): 154.

[5] Afsaneh Nahavandi and Ali R. Malekzadeh, "Acculturation in Mergers and Acquisitions," *Academy of Management Review* 3, no. 1 (1998): 82.

[6] E-mail from Intelligence Community official to the author, November 27, 2007. Name of Intelligence Community official withheld by mutual agreement.

benefits for all – an exchange of expertise as well as an exchange of cultures that allow all to embrace why organizations act as they do.

This idea of exchanging personnel has been employed in the more than fifty state and local intelligence fusion centers across the nation. In the Fusion Center Guidelines written collaboratively by DHS and the Department of Justice, a fusion center is defined as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[7] Fusion centers embrace the role of leveraging the available resources of all levels of government to "safeguard the homeland and prevent criminal activity."[8] Fusion centers also offer stakeholders the opportunity to communicate face to face and develop the personal relationships needed to build trust.

The National Governors Association recommends the intelligence fusion center as one of the ten key points to consider to strengthen a state's security.[9] As with state homeland security organizations, the state and local intelligence fusion centers across the nation are not identical. Each represents the varied approaches to homeland security taken by states and local jurisdictions. The majority of the fusion centers are led by a law

---

[7] U.S. Department of Justice, Office of Justice Programs, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, http://it.ojp.gov/documents/fusion_center_guidelines.pdf (accessed October 12, 2007), 2.

[8] U.S. Department of Justice, *Fusion Center Guidelines*, 4.

[9] National Governors Association Center for Best Practices, "A Governor's Guide to Homeland Security," http://www.nga.org/Files/pdf/0703GOVGUIDEHS.PDF (accessed September 3, 2007), 54.

enforcement entity such as the state police. The size of the fusion center staffs vary from three to about 250 with an average staff size of twenty-seven.[10]

The fusion center concept has been well-received at all levels of the homeland security community. This is primarily because all organizations benefit from this construct. One of the main benefits is the improved information flow from DHS to state and local governments and vice versa. Cathy Lanier, Chief of the Metropolitan Police Department, Washington DC, believes that the fusion centers "will help bridge some [of] the intelligence sharing gaps… by having analysts from different agencies and perspectives talking to each other and working together."[11] Andrew Lauland, Maryland Homeland Security Advisor, also sees the benefit of the fusion center concept stating "Collocation builds personal contacts and leverages different expertise in personnel… We are sharing collection, analysis, and production. We need to overcome cultural barriers [but] we are much better than before 9/11."[12]

In June 2006, the Secretary of Homeland Security designated the Office of Intelligence and Analysis[13] as the executive agent to manage the effort of improving the information flow between the fusion centers and DHS. The Office of Intelligence and Analysis' approach is to "deploy DHS personnel with operational and intelligence skills to the fusion centers to facilitate coordination and the flow of information between DHS

---

[10] U.S. Library of Congress, Congressional Research Service, *Fusion Centers: Issues and Options for Congress*, by Todd Masse, Siobhan O'Neil, and John Rollins, CRS RL34070 (July 6, 2007) http://fas.org/sgp/crs/intel/RL34070.pdf (accessed January 18,2008), 34.

[11] House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Over-classification and Pseudo-classification: The Impact on Information Sharing*, 110th Cong., 1st sess., March 22, 2007, http://homeland.house.gov/SiteDocuments/20070322121619-60472.pdf (accessed December 9, 2007).

[12] Andrew Lauland, interview by author, Annapolis, MD, January 8, 2008.

[13] Formerly known as the Office of Information Analysis

and the center."[14] DHS currently has 17 intelligence analysts assigned at fusion centers with a goal of 35 by the end of FY2008. The FBI has personnel at approximately 75% of the fusion centers.[15] While the percentage of federal personnel is small at the fusion centers, they can provide great benefit. Lt. Robin Taylor of the Maryland State Police and Watch Section Commander at the Maryland Coordination and Analysis Center (MCAC) recognized the benefits of federal personnel at the MCAC stating that by "having DHS and FBI here at the center, we have a federal rep that can find the answer. They come in and give you what you need."[16] In May 2007, Wayne Parent, Deputy Director of the DHS Office of Operations Coordination, testified that the Tennessee Office of Homeland Security adopted HSIN as "the backbone of its new state fusion center and recommended that all states adopt the network for information sharing and situational awareness."[17] If a close working relationship between DHS and the fusion centers enables better information sharing through the use of HSIN, then the benefits of building contacts and trust through the exchange of personnel has been valuable.

While the fusion center concept has improved coordination and information flow, the future is not clear for the fusion center. To date, states have relied on both state funds and funding from the Homeland Security Grant Program to establish and operate their

---

[14] U.S. Government Accountability Office, *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*, GAO-08-35. http://www.gao.gov/new.items/d0835.pdf (accessed December 9, 2007), 9.

[15] U.S. Library of Congress, CRS RL34070, 47 and U.S. Government Accountability Office, GAO-08-35, 20.

[16] Robin Taylor, interview by author, Woodlawn, MD, January 29, 2008.

[17] House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Fixing the Homeland Security Information Network: Finding the Way Forward For Better Information Sharing*, 110th Cong., 1st sess., May 10, 2007, http://homeland.house.gov/SiteDocuments/20070510132347-84079.pdf (accessed October 27, 2007), 5.

fusion centers. As the fusion centers reach maturity, initial successes will be forgotten and individual states will expect value from their fusion centers. Without tangible value, state funding for the fusion center may be eliminated. If the federal government reduces or ceases to provide fusion center sustainment funding; the focus of the fusion center, if it continues to operate, may not include federal homeland security issues. This uncertainty places a method of sustained culture change and improved information sharing at risk.

To make these culture-changing techniques effective, leadership must ensure that adequate time is given to "build a new generation that embraces the new culture."[18] Often, the behaviors are temporary because they are "subject to degradation as soon as pressures associated with a change effort are removed."[19] The leadership within the homeland security community must play a key role to maintain the behaviors that will drive a new culture. A mission-focused, collaborative culture is key to the effectiveness of HSIN and the successful execution of the homeland security mission. Current leadership in DHS understands the importance of eliminating the cultural differences that impede information sharing. Their priorities have been articulated and demonstrated to their employees through efforts to improve the HSIN program and in training programs designed to build critical skills for the homeland security mission. Continued support for the state and local intelligence fusion centers remains essential for the cultural changes to become enduring. As fusion centers operate for longer periods of time, more personnel come in contact with personnel from other agencies. These working relationships build trust and effect real culture change as the employees take these new behaviors, values, and assumptions learned at the fusion centers back to their parent agencies.

---

[18] John P. Kotter, *Leading Change* (Boston: Harvard Business School Press, 1996), 14.

[19] Kotter, 14.

VI. Conclusion

HSIN has struggled since its inception as a DHS program. It has been impacted by the law, programmatic issues, and the different cultures of the homeland security community. The Director of National Intelligence, Mike McConnell, has recognized the need to transform the culture of the Intelligence Community to "capture the benefits of collaboration… without destroying unique perspectives and capabilities."[1] The Homeland Security Advisory Council's Homeland Security Culture Task Force echoed these sentiments. To be effective, information sharing and collaboration must be part of the overarching culture.

To gauge the benefit of mitigating the cultural differences within the homeland security community that affect HSIN, Metcalfe's Law can be applied to describe the potential value of the network. Metcalfe's Law states that the potential value of a network increases as a function of the square of the number of nodes that are connected by the network.[2] The usefulness of the information on the network is impacted by the information's relevance, accuracy, and timeliness but the value of the network increases tremendously if more users are connected and exchanging information. HSIN has far greater potential and utility when connecting a large number of users that contribute and use information via the network than as just another "information sharing system." For example, the addition of two percent of all local governments to HSIN represents an

---

[1] Mike McConnell, "Overhauling Intelligence," *Foreign Affairs* 86, no. 4 (July/August 2007) under "Come Together," http://www.foreignaffairs.org/20070701faessay86404/mike-mcconnell/overhauling-intelligence.html (accessed December 6, 2007).

[2] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, DC: CCRP Publication Series, 2003), 250.

increase of three orders of magnitude in value over a network operating strictly at the state level.

In January 2008, DHS announced that the Homeland Security Information Network is being upgraded to address concerns regarding utility and duplication of capabilities. Reports of this announcement highlighted the criticism aimed at the department's effectiveness in satisfying the fundamental requirement to improve homeland security information sharing across all levels of government.[3] Regardless of the plans to change HSIN, the cultural differences that plagued the original HSIN must be addressed to build a mission-focused culture that fosters trust among the users of HSIN.

Through the discussion of HSIN problems and their underlying causes, the value of the state and local intelligence fusion centers has become apparent. The fusion center concept existed before 9/11 but gained real momentum shortly thereafter. Many state and local jurisdictions have established, staffed, and supported intelligence fusion centers to add value to the information sharing process. The fusion centers have not only provided benefit through connectivity and access to HSIN and its information from all levels of government but also through access to personnel from throughout the homeland security community including the FBI and DHS. The exchange of personnel has begun the process of building trust among the fusion center personnel. As a common purpose and trust are established among different organizations, the building of a new homeland security culture begins. With this shared homeland security vision, employing tools like HSIN will be expected. Culture change will take place slowly as relationships and trust are built and behaviors change. Leadership must remain vigilant to ensure that the new

[3] Spencer S. Hsu and Robert O'Harrow Jr., "DHS to Replace 'Duplicative' Anti-Terrorism Data Network," *Washington Post*, January 18, 2008.

behaviors become rooted in the shared values and assumptions of the homeland security community.

Leadership from the local, state, and federal level must maintain the focus of working collaboratively to prosecute the homeland security mission of preventing acts of terrorism in the U. S. and reducing America's vulnerability to terrorism. Today's dynamic environment requires leveraging all available capabilities and resources. HSIN in its current form is capable of assisting with the homeland security mission. Will the barriers of culture and longstanding beliefs remain, restricting the use of HSIN or will these barriers be removed? To see the complete security picture based on various sources, First Sergeant Lee Miller said "we must have an IT mechanism as well as trusted relationships to put these pieces together."[4] HSIN's future success is all about the people of the homeland security community adapting their organizations so they can leverage the information developed at the local, state, and federal levels. The citizens of this nation deserve the effort needed to change the organizational cultures of the homeland security community so HSIN can fulfill its intended function.

[4] House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Fixing the Homeland Security Information Network: Finding the Way Forward For Better Information Sharing*, 110th Cong., 1st sess., May 10, 2007, http://homeland.house.gov/SiteDocuments/20070510132259-40476.pdf (accessed November 30, 2007).

Bibliography

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: CCRP Publication Series, 2003.

Alberts, David S., and Richard E. Hayes. *Understanding Command and Control*. Washington, DC: CCRP Publication Series, 2006.

Blanchard, Benjamin B., and Wolter J. Fabrycky. *Systems Engineering and Analysis*. 3rd ed. Upper Saddle River, NJ: Prentice Hall, 1998.

Cartwright, Susan, and Cary L. Cooper, "The Role of Culture Compatibility in Successful Organizational Marriage," *Academy of Management Executive* 7, no. 2 (May 1993): 57-69.

Center for Strategic and International Studies. "Intelligence Reform and Terrorism Prevention Act of 2004." http://www.csis.org/media/csis/pubs/041201_irtpa_overview.pdf (accessed August 4, 2007).

Chang, Nancy. "The USA PATRIOT Act: What's So Patriotic About Trampling on the Bill of Rights?" In *Homeland Security and Terrorism : Readings and Interpretations*, edited by Russell D. Howard, James J. F. Forest, and Joanne C. Moore, 369-383. New York: McGraw-Hill, 2006.

Deal, Terrence E., and Allan A. Kennedy. *Corporate Cultures : The Rites and Rituals of Corporate Life*. Reading, Mass.: Addison-Wesley Pub. Co., 1982.

Electronic Frontier Foundation. "EFF Analysis Of The Provisions of the USA PATRIOT Act." http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php (accessed November 25, 2007).

Golden, Roger Dean. "What Price Security? The USA PATRIOT Act and America's Balance Between Freedom and Security." In *Homeland Security and Terrorism : Readings and Interpretations*, edited by Russell D. Howard, James J. F. Forest, and Joanne C. Moore, 400-412. New York: McGraw-Hill, 2006.

Graham, Saxon. *American Culture; An Analysis of Its Development and Present Characteristics*. New York: Harper, 1957.

Harrison, Roger. "Understanding Your Organization's Character," *Harvard Business Review* 50, no. 3 (May/June 1972): 119-128.

Hook, Brian H., Margaret J. A. Peterlin, and Peter L. Welsh. "The USA PATRIOT Act and Information Sharing Between the Intelligence and Law Enforcement Communities." In *Homeland Security and Terrorism : Readings and Interpretations*, edited by Russell D. Howard, James J. F. Forest, and Joanne C. Moore, 384-399. New York: McGraw-Hill, 2006.

Interoperability Clearinghouse Architecture Resource Center. "Homeland Security Enterprise Architecture." http://www.ichnet.org/IAC%201252003.ppt (accessed July 31, 2007).

Keating, Frank. "Catastrophic Terrorism: Local Response to a National Threat" In *Homeland Security and Terrorism : Readings and Interpretations*, edited by Russell D. Howard, James J. F. Forest, and Joanne C. Moore, 259-265. New York: McGraw-Hill, 2006.

Kettl, Donald F. *System Under Stress : Homeland Security and American Politics*. Washington, D.C.: CQ Press, 2004.

Kenyon, Henry S., Maryann Lawlor, and Cheryl Lilie. "Breaking Down Barriers to Homeland Security." *Signal* 58, no. 9 (May 2004): 75-77.

Kilmann, Ralph H. "Five Steps for Closing Culture-Gaps." In *Gaining Control of the Corporate Culture*. ed. Ralph H. Kilmann, Mary J. Saxton, and Roy Serpa, 351-369. San Francisco: Jossey-Bass Publishers, 1985.

Kostal, Devlin. "British Military Intelligence-Law Enforcement Integration in the Irish War of Independence, 1919-1921." In *Can't We All Get Along? Improving The Law Enforcement-Intelligence Community Relationship*, 117-142. Washington, DC: NDIC Press, 2007.

Kotter, John P. *Leading Change*. Boston: Harvard Business School Press, 1996.

Kotter, John P., and James L. Heskett. *Corporate Culture and Performance*. New York: The Free Press, 1992.

McConnell, Mike. "Overhauling Intelligence." *Foreign Affairs* 86, no. 4 (July/August 2007). http://www.foreignaffairs.org/20070701faessay86404/mike-mcconnell/overhauling-intelligence.html (accessed December 8, 2007).

McEntire, Marjorie H., and Joseph C. Bentley. "When Rivals Become Partners: Acculturation in a Newly-Merged Organization." *International Journal of Organizational Analysis* 4, no. 2 (April 1996): 154-174.

Nahavandi, Afsaneh, and Ali R. Malekzadeh, "Acculturation in Mergers and Acquisitions." *Academy of Management Review* 3, no. 1 (January 1998): 79-90.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report Executive Summary*. http://www.9-11commission.gov/report/911Report_Exec.pdf (accessed September 9, 2007).

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. http://www.9-11commission.gov/report/911Report.pdf (accessed September 9, 2007).

National Governors Association Center for Best Practices. "2006 State Homeland Security Directors Survey." http://www.nga.org/Files/pdf/0703GOVGUIDEHS.PDF (accessed September 3, 2007).

National Governors Association Center for Best Practices. "A Governor's Guide to Homeland Security." http://www.nga.org/Files/pdf/0703GOVGUIDEHS.PDF (accessed September 3, 2007).

Robbins, Stephen P. *Organizational Behavior: Concepts, Controversies, Applications*. 8th ed. Upper Saddle River, NJ: Prentice Hall, 1998.

Rollis, Devin. "The Wall Between National Security and Law Enforcement." In *Can't We All Get Along? Improving The Law Enforcement-Intelligence Community Relationship,* 143-162. Washington, DC: NDIC Press, 2007.

Russell, Richard A. "Department of Homeland Security: Information Sharing." Keynote presentation, 2004 Symposium on Integrated Justice Information Systems Supporting the Homeland, Washington DC, March 22, 2004.

http://www.search.org/conferences/2004symposium/presentations/monday/homeland.ppt (accessed August 2, 2007).

Schein, Edgar H., *Organizational Culture and Leadership*. San Francisco: Jossey-Bass, 2004.

U.S. Congress. House. Committee on Homeland Security. *The Homeland Security Information Network: An Update on DHS Information Sharing Efforts: Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment of the Committee on Homeland Security.* 109th Cong., 2d sess., September 13, 2006. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_house_hearings&docid=f:35623.pdf (accessed September 2, 2007).

U.S. Congress. House. Committee on Homeland Security. Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. *Fixing the Homeland Security Information Network: Finding the Way Forward For Better Information Sharing*, 110th Cong., 1st sess., May 10, 2007. http://homeland.house.gov/SiteDocuments/20070510132259-40476.pdf (accessed November 30, 2007).

U.S. Congress. House. Committee on Homeland Security. Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. *Fixing the Homeland Security Information Network: Finding the Way Forward For Better Information Sharing*, 110th Cong., 1st sess., May 10, 2007. http://homeland.house.gov/SiteDocuments/20070510132347-84079.pdf (accessed October 27, 2007).

U.S. Congress. House. Committee on Homeland Security. Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. *Over-classification and Pseudo-classification: The Impact on Information Sharing*, 110th Cong., 1st sess., March 22, 2007, http://homeland.house.gov/SiteDocuments/20070322121619-60472.pdf (accessed December 9, 2007).

U.S. Congress. House. Permanent Select Committee on Intelligence. *Report of the Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001.* 107th Cong., 2d sess., December 2002. http://www.gpoaccess.gov/serialset/creports/pdf/fullreport_errata.pdf (accessed November 17, 2007).

U.S. Department of Defense. *Defense Acquisition Guidebook.* https://akss.dau.mil/dag/GuideBook/PDFs/Chapter_4.pdf (accessed December 6, 2007).

U.S. Department of Homeland Security. *Department of Homeland Security Fiscal Year 2007 Annual Financial Report,"* http://www.dhs.gov/xlibrary/assets/cfo_afrfy2007.pdf. (accessed November 25, 2007).

U.S. Department of Homeland Security. *Homeland Security Information Network.* http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm (accessed September 9, 2007).

U.S. Department of Homeland Security. Homeland Security Advisory Council. *Report of the Culture Task Force, January 2007*. http://www.dhs.gov/xlibrary/assets/hsac-culture-010107.pdf (accessed September 1, 2007).

U.S. Department of Homeland Security. Office of the Inspector General. *Homeland Security Information Network Could Support Information Sharing More Effectively OIG-06-38*. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_06-38_Jun06.pdf (accessed August 10, 2007).

U.S. Department of Justice. Office of Justice Programs. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. http://it.ojp.gov/documents/fusion_center_guidelines.pdf (accessed October 12, 2007).

U.S. Executive Office of the President. "Analysis for the Homeland Security Act of 2002." http://www.whitehouse.gov/deptofhomeland/analysis/hsl-bill-analysis.pdf (accessed September 16, 2007).

U.S. General Accounting Office. *High-Risk Series: An Update*. GAO-03-119. http://www.gao.gov/pas/2003/d03119.pdf (accessed October 14, 2007).

U.S. General Accounting Office. *Organizational Culture: Techniques Companies Use to Perpetuate or Change Beliefs and Values*. GAO/NSIAD-92-105. http://archive.gao.gov/d31t10/146086.pdf (accessed August 11, 2007).

U.S. Government Accountability Office. *Enterprise Architecture: Leadership Remains Key to Establishing and Leveraging Architectures for Organizational*

Transformation. GAO-06-831. http://www.gao.gov/new.items/d06831.pdf (accessed July 31, 2007).

U.S. Government Accountability Office. *Homeland Security: DHS Enterprise Architecture Continues to Evolve but Improvements Needed.* GAO-07-564. http://www.gao.gov/new.items/d07564.pdf (accessed July 31, 2007).

U.S. Government Accountability Office. *Homeland Security: Efforts Under Way to Develop Enterprise Architecture, but Much Work Remains*. GAO-04-777. http://www.gao.gov/new.items/d04777.pdf (accessed July 31, 2007).

U.S. Government Accountability Office. *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers*. GAO-08-35. http://www.gao.gov/new.items/d0835.pdf (accessed December 9, 2007).

U.S. Government Accountability Office. *Information Technology: Major Federal Networks That Support Homeland Security Functions.* GAO-04-375. http://www.gao.gov/new.items/d04375.pdf (accessed September 2, 2007).

U.S. Government Accountability Office. *Information Technology Homeland Security Information Network Needs to Be Better Coordinated with Key State and Local Initiatives.* GAO-07-822T. http://www.gao.gov/new.items/d07822t.pdf (accessed August 2, 2007).

U.S. Joint Forces Command. *Noble Resolve 07-1 yields new opportunities for experimentation*. http://www.jfcom.mil/newslink/storyarchive/2007/pa053107.html (accessed March 30, 2008).

U.S. Library of Congress. Congressional Research Service. *Fusion Centers: Issues and Options for Congress* by Todd Masse, Siobhan O'Neil, and John Rollins, CRS RL34070 (July 6, 2007) http://fas.org/sgp/crs/intel/RL34070.pdf (accessed January 18,2008).

U.S. Library of Congress. Congressional Research Service. *Sharing Law Enforcement and Intelligence Information: The Congressional Role* by Richard A. Best Jr. CRS RL33873 (February 13, 2007) http://www.fas.org/sgp/crs/intel/RL33873.pdf (accessed August 4, 2007).

U.S. Office of the Director of National Intelligence. Office of the Program Manager-Information Sharing Environment. *Information Sharing Environment Implementation Plan*. http://www.ise.gov/docs/reports/ise-impplan-200611.pdf (accessed February 9, 2008).

U.S. Office of Management and Budget. *Circular A-11, Part 7, Planning, Budgeting, Acquisition, and Management of Capital Assets.* http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf (accessed November 21, 2007).

U.S. Office of Management and Budget. Federal Enterprise Architecture Program Management Office. *FEA Practice Guidance.* http://www.whitehouse.gov/omb/egov/documents/FEA_Practice_Guidance.pdf (accessed September 23, 2007).

U.S. President. Executive Order no. 13228, Code of Federal Regulations, title 3. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_cfr_3v1&docid=3CFR13228.pdf (accessed January 4, 2008) 796.

U.S. President. *National Strategy for Homeland Security*. http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf (accessed August 4, 2007).

Author Biography

Mr. Jeffery E. Bradey is a Department of Defense civilian. Prior to attending the Joint Advanced Warfighting School in Norfolk, Virginia, Mr. Bradey held various engineering, acquisition, and management positions in his tenure at the Department of Defense. Most recently, Mr. Bradey was an information technology manager at the Joint Defence Facility Pine Gap in Alice Springs, Australia. Prior to his assignment in Australia, Mr. Bradey was the engineering advisor in the Defense Attaché/Technical Liaison Office at the U.S. Embassy in Bangkok, Thailand. Mr. Bradey has a Bachelor of Science in Engineering from the University of South Carolina and a Master of Science in Electrical Engineering from Johns Hopkins University.